Notice to Proposers

This solicitation may be subject to the County's Wage Requirements law for service contracts. If this solicitation is subject to this law, then it will be indicated on the next page (page 1).

If this solicitation is subject to the Wage Requirements law, then the "Wage Requirements Certification" and, if applicable, the "501(c)(3) Nonprofit Organization's Employee's Wage and Health Insurance Form" (see Attachment E), must be completed and submitted with your proposal. If you fail to submit and complete the required material information on the form(s), your proposal is unacceptable under County law and will be rejected.

Please note the information pertaining to the Wage Requirements law is on Attachment E. Please note for services contracts, you can find the mandatory current per hour rate payable to employees under Section 11B-33A of the County Code by going to the website (www.montgomerycountymd.gov), and clicking on Departments, then on Procurement. Also, the Wage Requirements law is available at this website.

REQUEST FOR PROPOSALS
RFP #425820958
Professional Auditing Services

August 20, 2015

The Montgomery County Council, Montgomery County, Maryland is soliciting proposals for the provision of the above-referenced services as outlined in this document.

One original and seven (7) copies of your proposal must be submitted in a sealed envelope/package **no later than 3:00 p.m. on Friday, October 16, 2015** to the Office of Legislative Oversight, Council Office Building, 100 Maryland Avenue, Rockville, Maryland 20850-4166. The sealed proposal package must be clearly marked with the solicitation number, due date, and due time.

There will be an optional pre-submission conference at 2:00 p.m. on Thursday, September 10, 2015 in the 6th Floor Conference Room of the Council Office Building, 100 Maryland Avenue, Rockville, MD 20850.

The County **will not** accept fax proposals or proposals sent via e-mail. All faxed or e-mailed proposals will be returned.

Should you have any questions regarding the technical information or the scope of services contained in this solicitation, please contact Leslie Rubin in the Office of Legislative Oversight at (240) 777-7998.

This is a Services Contract (see Section A, Services Contract):	**X**

or

This is not a Services Contract (disregard Section A, Services Contract):	

TABLE OF CONTENTS

Acknowledgment 5

Name and Signature Requirements for Proposals and Contracts 5

Acknowledgment of Solicitation Amendments 5

Section A **Instructions, Conditions and Notices 6**
Acceptance Time
Acknowledgment
Confidential Information
Contract Documents
Contractor Staff
Council is the Principal Client
Determination of Responsibility
Issuing Office and Point of Contact
Joint Procurement
Late Proposals
Minority, Female, Disabled Person Program Compliance
Optional Pre-Submission Conference
Other Contracts with the County
Payment Terms
Proposals
Proposal Withdrawal/Modification
Proprietary & Confidential Information
Qualification of Offerors
Questions
Solicitation Amendments
Solicitation Preparation Expenses
Verbal Explanations
Verification and Audits
Wage Requirements

Section B **General Conditions of Contract Between County Council and Contractor 12**
Accounting System and Audit, Accurate Information
Americans with Disabilities Act
Applicable Laws
Assignments and Subcontracts
Changes
Contract Administration
Cost & Pricing Data
Disputes
Documents, Materials and Data
Duration of Obligation
Entire Agreement

TABLE OF CONTENTS (continued)

Ethics Requirements/Political Contributions
Guarantee
Hazardous and Toxic Substances
Health Insurance Portability and Accountability Act (HIPPA) Compliance
Immigration Reform and Control Act
Inconsistent Provisions
Indemnification
Independent Contractor
Inspections
Insurance
Intellectual Property Approval and Indemnification – Infringement
Non-Conviction of Bribery
Non-Discrimination in Employment
Payments
Personal Property
Protection of Personal Information by Government Agencies
Termination for Default
Termination for Convenience
Time
Work Under The Contract
Workplace Safety

Section C **Scope of Services** **22**
Background
Intent
Work Statement
Deliverables
Offeror Qualifications
Contractor Responsibility
County Responsibility
Montgomery County Union Employees Deferred Compensation Plan Responsibility

Section D **Performance Period** **32**
Term
Price Adjustments

Section E **Method of Award/Evaluation Criteria** **33**
Procedures
Evaluation Criteria

Section F **Proposal Submissions** **35**

Section G **Compensation** **38**

Section H **Contract Administrator** **38**

Section I **Ethics** **38**

Section J **Computer Resources Security** **39**

TABLE OF CONTENTS (continued)

ATTACHMENTS

A. References A1

B. Minority-Owned Business Addendum to the General Conditions of Contract Between County and Contractor, and its companion document entitled "Minority, Female, Disabled Person Subcontractor Performance Plan" B1

C. Offeror's Certification of Cost and Price C1

D. Mandatory Insurance Requirements D1

E. Wage Requirements for Services Contracts Addendum to The General Conditions of Contract between County Council and Contractor E1

F. Price Sheets F1

G. Business Associate Agreement G1

H. Administrative Procedures 6-1 and 6-7 ..... H1

RFP #425820958

Montgomery County, Maryland

Acknowledgment Page

ACKNOWLEDGMENT

The Offeror must include a signed acknowledgment that all the terms and conditions of the offer may, at the County Council's option, be made applicable in any contract issued as a result of this solicitation. Offers that do not include such an acknowledgment may be rejected. Executing and returning (with the offer) the acknowledgment shown below may satisfy this requirement.

The undersigned agrees that all the terms and conditions of this solicitation and offer may, at the County Council's option, be made applicable in any contract issued as a result of this solicitation.

Business Firm's Typed Name: _____

Name and Title of Person
Authorized to Sign Proposal: _____

Signature: _____ Date: _____

Corporate Attestation or SEAL *here*

Signature: _____ Date: _____
(Corporate officer other than above)

Name and Title of Person
Attesting to Authorized Signature: _____

NAME AND SIGNATURE REQUIREMENTS FOR PROPOSALS AND CONTRACTS

The correct legal business name of the Offeror must be used in all contracts. A trade name (i.e., a shortened or different name under which the firm does business) should not be used when the legal name is different. Corporations must have names that comply with State Law. The Offeror's signature must conform to the following:

- Where the Offeror is a corporation, a corporate seal is required and the Contract must be signed by an Officer of the Corporation who possesses the authority to sign contracts for the Corporation.
- Where the Offeror is a partnership, at least one general partner must sign.
- Where the Offeror is a sole proprietor, the owner of the company must sign.

By submitting a proposal under this Solicitation, the Offeror agrees that the Montgomery County Council has 120 days after the due date in order to accept the proposal.

ACKNOWLEDGMENT OF SOLICITATION AMENDMENTS

The Offeror acknowledges receipt of the following amendment(s) to the solicitation:

Amendment Number	Date

SECTION A - INSTRUCTIONS, CONDITIONS AND NOTICES

The following provisions are applicable to this solicitation:

1. ACCEPTANCE TIME

By submitting a proposal under this solicitation, the Offeror agrees that the Montgomery County Council has 120 days after the due date in order to accept the proposal. The County Council reserves the right to reject, as unacceptable, any offer that specifies less than 120 days of acceptance time. Upon mutual agreement between the County Council and the Offeror, the acceptance time for the Offeror's proposal may be extended.

2. ACKNOWLEDGMENT

The Offeror is to include a signed acknowledgment indicating agreement with all the terms and conditions of the solicitation.

3. CONFIDENTIAL INFORMATION

Some material to be reviewed by the Contractor in performance of a contract will be of a confidential or proprietary nature. The Contractor must enter into a Business Associate Agreement with the County Council, which addresses access to protected health information as defined in the Health Insurance Portability and Accountability Act (HIPAA). See Attachment page G1. In addition, the Contractor may be required to sign confidentiality agreements with third-party providers of County data.

The Contractor must not divulge such confidential or proprietary information to any party other than the County Council or other County officials directly involved in the audit and must comply with the confidentiality standards for client information established by the American Institute of CPAs (AICPA).

4. CONTRACT DOCUMENTS

The following documents will be incorporated into the contract resulting from this solicitation:

a. General Conditions of Contract Between County Council & Contractor,
b. Minority Business Program & Offeror's Representation,
c. Minority-Owned Business Addendum to the General Conditions of Contract Between County Council & Contractor,
d. Minority, Female, Disabled Person Subcontractor Performance Plan, and
e. Offeror's Certification of Cost & Price (for contracts above $100,000).

5. CONTRACTOR STAFF

Key personnel (partner, managers, supervisors, and seniors) of the Contractor's staff will be expected to work at the level of effort proposed by the Contractor unless a change is authorized by the Office of Legislative Oversight. The Contractor must notify the Contract Administrator in writing if it becomes necessary to replace any of the key personnel. The Contractor must provide the resumes for new personnel assigned to the work, and the new personnel's qualifications and experience must be at least equal to those of the replaced staff. The Contract Administrator must approve the personnel change in writing prior to the change taking place.

SECTION A - INSTRUCTIONS, CONDITIONS AND NOTICES (continued)

6. COUNCIL IS THE PRINCIPAL CLIENT

Section 315 of the Montgomery County Charter states:

> "The Council shall contract with, or otherwise employ, a certified public accountant to make annually an independent post-audit of all financial records and actions of the County, its officials and employees. The complete report of the audit shall be presented to the Council and copies of it shall be made available to the public."

The County Council is the principal client and as such will enter into written contracts with the firm selected to perform auditing services. The Council, through the Audit Committee, must be kept fully informed of any problems and issues arising during the course of any audits, as well as progress being made toward the completion of the audits.

7. DETERMINATION OF RESPONSIBILITY

The Offeror has the burden of demonstrating affirmatively its responsibility in connection with this solicitation. A debarred potential Offeror must automatically be considered non-responsible in connection with this solicitation. The County Council reserves the right to consider an Offeror non-responsible who has previously failed to perform properly or to complete, in a timely manner, contracts of a similar nature, or if investigation shows the Offeror unable to perform the requirements of the contract.

An Offeror may be requested at any time by the Director, Office of Legislative Oversight to provide additional information, references and other documentation and information that relate to the determination of responsibility. Failure of an Offeror to furnish requested information may constitute grounds for a finding of non-responsibility of the prospective Offeror.

The County Council may deny the award, renewal, or assignment of a contract to or for any Offeror who is in default of payment of any money due the County.

The factors that may be considered in connection with a determination of responsibility include:

a. The ability, capacity, organization, facilities, and skill of the Offeror to perform the contract or provide the goods or services required;
b. The ability of the Offeror to perform the contract or provide the services within the time specified without delay, interruption, or interference;
c. The integrity, reputation, and experience of the Offeror, and its key personnel;
d. The quality of performance of previous contracts or services for the County or other entities. Past unsatisfactory performance, for any reason, is sufficient to justify a finding of non-responsibility;
e. The sufficiency of financial resources of the Offeror to perform the contract or provide the services;
f. The certification of an appropriate accounting system, if required by the contract type;
g. A bid bond and the Offeror's evidence of ability to furnish a performance bond may be considered evidence of responsibility; and
h. Past debarment by the County or other entity.

8. ISSUING OFFICE AND POINT-OF-CONTACT

This Request for Proposal (RFP) is issued by the Montgomery County Council's Audit Committee on behalf of the County Council. The person identified below has the responsibility and authority to perform the functions of the Contact Administrator for this Contract.

SECTION A - INSTRUCTIONS, CONDITIONS AND NOTICES (continued)

Name: Leslie Rubin
Title: Audit Contract Administrator
Address: Office of Legislative Oversight
Council Office Building
100 Maryland Avenue, Room 509
Rockville, Maryland 20850-4166
Telephone: (240) 777-7998

During any prolonged absence of the designated Contract Administrator, the Director of the Office of Legislative Oversight will serve as the alternate Contract Administrator. Unless the Council President changes this delegation of authority, in writing, no other person is authorized to perform the functions of the Contract Administrator for this Contract.

9. JOINT PROCUREMENT

The following entities within Montgomery County must be able to purchase directly from any contracts resulting from this solicitation:

Maryland-National Capital Park & Planning Commission (M-NCPPC)
Montgomery Community College (MCC)
Montgomery County Public Schools (MCPS)
Montgomery County Revenue Authority
Montgomery County Housing Opportunities Commission (HOC)
Washington Suburban Sanitary Commission (WSSC)
Municipalities & Special Tax Districts in Montgomery County
Montgomery County Economic Development Corporation

While this solicitation is prepared on behalf of the Legislative Branch of Montgomery County, it is intended to apply for the benefit of the Executive Branch of Montgomery County and the above-named entities as though they were expressly named throughout the document. Each of these entities may purchase from the successful Offeror under the same prices and terms of services of the contract with the County Council, in accordance with each entity's respective laws and regulations, or an entity may choose not to procure from the successful Offeror at the entity's sole discretion. If the Executive Branch or one of the above-named entities elects to purchase under the contract, the price shall be determined by using unit costs and other pertinent costs that are provided in the offer. Montgomery County Government shall not be held liable for any costs, payments, or damages incurred by the above jurisdictions.

If a service currently provided by Montgomery County or by any above-named entities is the subject of legislation that creates a new legal entity to provide the service, the new legal entity also may purchase from the successful Offeror under the same prices and terms of services of the contract with the County Council as if they were an above-named entity.

10. LATE PROPOSALS

Responses to this solicitation received after the date and time specified in the solicitation are considered late and may not, under any circumstances, be considered for any award resulting from the solicitation.

11. MINORITY, FEMALE, DISABLED PERSON PROGRAM COMPLIANCE

While this solicitation is exempt from Montgomery County procurement laws and regulations pursuant to County Code §11B-4(a)(3), the Offeror must comply with the requirements of the Minority-Female-Disabled Person (MFD) procurement program. Further information regarding the County's MFD program is contained within this solicitation (see Attachment B entitled "Minority-owned Business Addendum to General Conditions of Contract between County Council and Contractor" and its companion document entitled "Minority, Female, Disabled Person Subcontractor Performance Plan").

SECTION A - INSTRUCTIONS, CONDITIONS AND NOTICES (continued)

12. OPTIONAL PRE-SUBMISSION CONFERENCE

An optional Pre-Submission Conference will be held on Thursday, September 10, 2015 at 2 p.m. in the 6th Floor Conference Room of the Council Office Building, 100 Maryland Avenue, Rockville, MD 20850. Although optional, it is highly recommended that prospective Offerors attend the Pre-Submission Conference.

13. OTHER CONTRACTS WITH THE COUNTY

Any additional work during the period of any contract that the selected firm or its affiliates propose to perform for Montgomery County, Maryland, over and above the auditing services specified in this RFP will be subject to the prior written concurrence of the County Council. The concurrence will be expressed through the Audit Committee after verifying that there is no conflict of interest or unfair advantage.

14. PAYMENT TERMS

The County's payment terms are net thirty (30) days.

15. PROPOSALS

Sealed proposals are due by 3:00 p.m. on Friday, October 16, 2015 in the Office of Legislative Oversight, Council Office Building, 100 Maryland Avenue, Room 509, Rockville, Maryland 20850-4166, for the purchase of services in accordance with the instructions, terms, conditions and work statement (scope of services) set forth in this solicitation. Proposals must be returned in a sealed envelope, and clearly marked with the RFP number, due date, and time. Proposals received after the time specified will be returned unopened to the Offeror. The County Council will not be responsible for proposals received after the due date, due to premature or late deliveries, postal/courier delays, or opening of a proposal if it is improperly addressed or identified.

16. PROPOSAL WITHDRAWAL/MODIFICATION

Proposals may be withdrawn or may be modified by the Offeror upon receipt of a written request received before the time specified for due date and due time. Requests to withdraw or modify an Offeror's proposal received after the solicitation due date and time will not be considered.

17. PROPRIETARY & CONFIDENTIAL INFORMATION

This is to notify prospective Offerors that the County Council has unlimited data rights regarding proposals submitted in response to its solicitations. Unlimited data rights mean that the County Council has the right to use, disclose, reproduce, prepare derivative works, distribute copies to the public, or perform publicly and display publicly any information submitted by Offerors in response to this or any solicitation issued by the County Council. However, information that is deemed to be confidential commercial or financial information as defined by the Maryland Information Act, State Government Article 10-617 will be exempted from disclosure if theOfferor can show that release of such information would cause substantial competitive harm to the Offeror's competitive position. It is the responsibility of the Offeror to clearly identify each part of his/her offer that is confidential commercial or financial information by stamping the bottom right-hand corner of each pertinent page with one inch bold face letters stating the words "confidential" or "proprietary." The Offeror agrees that any portion of the proposal that is not stamped as proprietary or confidential will be deemed not to be proprietary or confidential.

SECTION A - INSTRUCTIONS, CONDITIONS AND NOTICES (continued)

18. QUALIFICATION OF OFFERORS

Offerors may be required to furnish satisfactory evidence that they are qualified and regularly engaged in performing the services for which they are submitting a proposal and maintain a regularly established place of business. An authorized representative of the County Council may visit any Offeror's plant, place of business or place where the services are performed to determine ability, capacity, reliability, financial stability and other factors necessary to perform the contract. If so requested, an Offeror may be required to submit information about its reputation, past performance, business and financial capability and other factors that demonstrate that the Offeror is capable of satisfying the County Council's needs and requirements for a specific contract.

19. QUESTIONS

All technical and non-technical questions pertaining to this solicitation should be directed to the individual whose name appears on the Request For Proposal cover sheet.

20. SOLICITATION AMENDMENTS

In the event that an amendment to this solicitation is issued, all solicitation terms and conditions will remain in effect unless they are specifically changed by the amendment. Offerors must acknowledge receipt of such solicitation amendments, to the place designated, and prior to the hour and date specified in the solicitation (or as amended) for receipt of offers. Offerors may acknowledge solicitation amendments by one of the following:

a. By returning one signed copy of the amendment either with your Proposal or by sending it separately to the Office of Legislative Oversight.

b. By acknowledging receipt of the amendment on the Acknowledgment (see page 5) submitted.

c. By stating that the amendment is acknowledged in a signed letter that refers to the solicitation and amendment numbers.

21. SOLICITATION PREPARATION EXPENSES

All costs incurred in the preparation and submission of solicitations will be borne by the Offeror and shall not be incurred in anticipation of receiving reimbursement from the County.

22. VERBAL EXPLANATIONS

Verbal explanations or instructions given by a Montgomery County employee to an Offeror in regard to this solicitation will not be binding on the County Council. Any information given to an Offeror in response to a request will be furnished to all Offerors as an amendment to this solicitation, if such information is deemed necessary for the preparation of solicitations, or if the lack of such information would be detrimental to the uninformed Offerors. Such amendments, only when issued by the Director, Office of Legislative Oversight, will be considered as being binding on the County.

23. VERIFICATION AND AUDITS

The Contractor and all subcontractors must maintain for a period of five years, books, records, documents, and other evidence directly pertinent to the performance of work under this contract ("audit documentation"), in accordance with appropriate accounting procedures and generally accepted government auditing standards. The Contractor must make audit documentation available, upon written request, in a timely manner to other auditors or reviewers in accordance with generally accepted government auditing standards. At the County's request, the Contractor must provide proper facilities within its offices during normal business hours, for purposes of making audit documentation available to such other auditors or reviewers.

24. WAGE REQUIREMENTS

While this solicitation is exempt from Montgomery County procurement laws and regulations pursuant to County Code § 11B-4(a)(3), the Offeror must comply with certain wage requirements payable to the Contractor's employees. Additional information regarding the County's wage requirements is contained within this solicitation (see Attachment E - "Wage Requirements for Services Contracts Addendum to The General Conditions of Contract between County Council and Contractor" and its companion document entitled "Wage Requirements Certification"). **If Contractor fails to submit and complete the required material information on the Wage Requirements Certification form, its proposal is considered unacceptable and will be rejected.**

END SECTION A - INSTRUCTIONS, CONDITIONS AND NOTICES

SECTION B - GENERAL CONDITIONS OF CONTRACT BETWEEN COUNTY COUNCIL & CONTRACTOR

1. ACCOUNTING SYSTEM AND AUDIT, ACCURATE INFORMATION

The contractor certifies that all information the contractor has provided or will provide to the County Council is true and correct and can be relied upon by the County Council in awarding, modifying, making payments, or taking any other action with respect to this contract including resolving claims and disputes. Any false or misleading information is a ground for the County Council to terminate this contract for cause and to pursue any other appropriate remedy. The contractor certifies that the contractor's accounting system conforms with generally accepted accounting principles, is sufficient to comply with the contract's budgetary and financial obligations, and is sufficient to produce reliable financial information.

Representatives of the County Council may examine the contractor's and any first-tier subcontractor's records to determine and verify compliance with the contract and to resolve or decide any claim or dispute arising under this contract. The contractor and any first-tier subcontractor must grant the representatives of the County Council access to these records at all reasonable times during the contract term and for 3 years after final payment. If the contract is supported to any extent with federal or state funds, the appropriate federal or state authorities may also examine these records. The contractor must include the preceding language of this paragraph in all first-tier subcontracts.

2. AMERICANS WITH DISABILITIES ACT

The contractor agrees to comply with the nondiscrimination requirements of Titles II and III, and other provisions, of the Americans with Disabilities Act of 1990, Pub. Law 101-336, and ADA Amendments Act of 2008, Pub. Law 110-325, as amended, currently found at 42 U.S.C., § 12101, et seq., and 47 U.S.C., ch. 5.

3. APPLICABLE LAWS

This contract must be construed in accordance with the laws and regulations of Maryland and Montgomery County. The contractor must, without additional cost to the County, pay any necessary fees and charges, obtain any necessary licenses and permits, and comply with applicable federal, state and local laws, codes and regulations. For purposes of litigation involving this contract, except for contract Disputes discussed in paragraph 8 below, exclusive venue and jurisdiction must be in the Circuit Court for Montgomery County, Maryland or in the District Court of Maryland for Montgomery County.

Furthermore, certain non-profit and governmental entities may purchase supplies and services, similar in scope of work and compensation amounts provided for in a County contract, using their own contract and procurement laws and regulations, pursuant to the Md. State Finance and Procurement Article, Section 13-101, et. seq**.**

Contractor and all of its subcontractors must comply with the provisions of County Code §11B-35A and must not retaliate against a covered employee who discloses an illegal or improper action described in §11B-35A. Furthermore, an aggrieved covered employee under §11B-35A is a third-party beneficiary under this Contract, who may by civil action recover compensatory damages including interest and reasonable attorney's fees, against the contractor or one of its subcontractors for retaliation in violation of that Section.

Contractor and all of its subcontractors must provide the same benefits to an employee with a domestic partner as provided to an employee with a spouse, in accordance with County Code §11B-33D. An aggrieved employee, is a third-party beneficiary who may, by civil action, recover the cash equivalent of any benefit denied in violation of §11B-33D or other compensable damages.

The contractor agrees to comply with the requirements of the Displaced Service Workers Protection Act, which appears in County Code, Chapter 27, Human Rights and Civil Liberties, Article X, Displaced Service Workers Protection Act,§§ 27-64 through 27-66.

4. ASSIGNMENTS AND SUBCONTRACTS

The contractor must not assign or transfer this contract, any interest herein or any claim hereunder, except as expressly authorized in writing by the County Council. Unless performance is separately and expressly waived in writing by the County Council, an assignment does not release the contractor from responsibility for performance of this contract. Unless otherwise provided in the contract, the contractor may not contract with any other party for furnishing any of the materials or services herein contracted for without the written approval of the County Council. Any subcontract for any work hereunder must comport with the terms of this Contract and County law, and must include any other terms and conditions that the County deems necessary to protect its interests.

5. CHANGES

The County Council may unilaterally change the work, materials and services to be performed. The change must be in writing and within the general scope of the contract. The contract will be modified to reflect any time or money adjustment the contractor is entitled to receive. Contractor must bring to the Contract Administrator, in writing, any claim about an adjustment in time or money resulting from a change, within 30 days from the date the County Council issued the change in work, or the claim is waived. Any failure to agree upon a time or money adjustment must be resolved under the "Disputes" clause of this contract. The contractor must proceed with the prosecution of the work as changed, even if there is an unresolved claim. No charge for any extra work, time or material will be allowed, except as provided in this section.

6. CONTRACT ADMINISTRATION

In accordance with the Montgomery County Code Section 29A-5(b)(9), the Office of Legislative Oversight (OLO) will administer the contract. The contract administrator, subject to paragraph B below, is the Office representative designated by the Director of OLO and is authorized to:

(a) serve as liaison between the County and the contractor;
(b) give direction to the contractor to ensure satisfactory and complete performance;
(c) monitor and inspect the contractor's performance to ensure acceptable timeliness and quality;
(d) serve as records custodian for this contract, including wage and prevailing wage requirements;
(e) accept or reject the contractor's performance;
(f) furnish timely written notice of the contractor's performance failures to the County Council and to the County Attorney, as appropriate;
(g) prepare required reports;
(h) approve or reject invoices for payment;
(i) recommend contract modifications or terminations to the County Council;
(j) issue notices to proceed; and
(k) monitor and verify compliance with any MFD Performance Plan.

The contract administrator is NOT authorized to make determinations (as opposed to recommendations) that alter, modify, terminate or cancel the contract, interpret ambiguities in contract language, or waive the County's contractual rights.

7. COST & PRICING DATA

Chapter 11B of the County Code and the Montgomery County Procurement Regulations require that cost & pricing data be obtained from proposed awardees/contractors in certain situations. The contractor guarantees that any cost & pricing data provided to the County Council will be accurate and complete. The contractor grants County Council representatives access to all books, records, documents, and other supporting data in order to permit adequate evaluation of the contractor's proposed price(s). The contractor also agrees that the price to the County Council, including profit or fee, may, at the option of the County Council, be reduced to the extent that the price was based on inaccurate, incomplete, or noncurrent data supplied by the contractor.

8. DISPUTES

Any dispute arising under this contract that is not disposed of by agreement must be decided under the Montgomery County Code and the Montgomery County Procurement Regulations. Pending final resolution of a dispute, the Contractor must proceed diligently with contract performance. Subject to subsequent revocation or alteration by the County Council, the head of the County department, office or agency ("Department Head") of the contract administrator is the designee of the County Council, for the purpose of dispute resolution. The Department Head, or his/her designee, must forward to the County Council a copy of any written resolution of a dispute. The Department Head may delegate this responsibility to another person (other than the contract administrator). A contractor must notify the contract administrator of a claim in writing, and must attempt to resolve a claim with the contract administrator prior to filing a dispute with the County Council. The contractor waives any dispute or claim not made in writing and received by the County Council within 30 days of the event giving rise to the dispute or claim, whether or not the contract administrator has responded to a written notice of claim or resolved the claim. The County Council must dismiss a dispute that is not timely filed. A dispute must be in writing, for specific relief, and any requested relief must be fully supported by affidavit of all relevant calculations, including cost and pricing information, records, and other information. At the County's option, the contractor agrees to be made a party to any related dispute involving another contractor.

9. DOCUMENTS, MATERIALS AND DATA

All documents materials or data developed as a result of this contract are the County's property. The County has the right to use and reproduce any documents, materials, and data, including confidential information, used in the performance of, or developed as a result of, this contract. The County may use this information for its own purposes, including reporting to state and federal agencies. The contractor warrants that it has title to or right of use of all documents, materials or data used or developed in connection with this contract. The contractor must keep confidential all documents, materials, and data prepared or developed by the contractor or supplied by the County.

10. DURATION OF OBLIGATION

The contractor agrees that all of contractor's obligations and warranties, including all requirements imposed by the Minority Owned Business Addendum to these General Conditions, if any, which directly or indirectly are intended by their nature or by implication to survive contractor performance, do survive the completion of performance, termination for default, termination for convenience, or termination by mutual consent of the contract.

11. ENTIRE AGREEMENT

There are no promises, terms, conditions, or obligations other than those contained in this contract. This contract supersedes all communications, representations, or agreements, either verbal or written, between the parties hereto, with the exception of express warranties given to induce the County Council to enter into the contract.

12. ETHICS REQUIREMENTS/POLITICAL CONTRIBUTIONS

The contractor must comply with the ethics provisions contained in Chapters 11B and 19A, Montgomery County Code, which include the following:

(a) a prohibition against making or offering to make certain gifts. Section 11B-51(a).
(b) a prohibition against kickbacks. Section 11B-51(b).
(c) a prohibition against a person engaged in a procurement from employing or offering to employ a public employee. Section 11B-52 (a).
(d) a prohibition against a contractor that is providing a recommendation to the County from assisting another party or seeking to obtain an economic benefit beyond payment under the contract. Section 11B-52 (b).
(e) a restriction on the use of confidential information obtained in performing a contract. Section 11B-52 (c).
(f) a prohibition against contingent fees. Section 11B-53.

Furthermore, the contractor specifically agrees to comply with Sections 11B-51, 11B-52, 11B-53, 19A-12, and/or 19A-13 of the Montgomery County Code.

In addition, the contractor must comply with the political contribution reporting requirements currently codified under the Election Law at Md. Code Ann., Title 14.

13. GUARANTEE

A. Contractor guarantees for one year from acceptance, or for a longer period that is otherwise expressly stated in the County Council's written solicitation, all goods, services, and construction offered, including those used in the course of providing the goods, services, and/or construction. This includes a guarantee that all products offered (or used in the installation of those products) carry a guarantee against any and all defects for a minimum period of one year from acceptance, or for a longer period stated in the County Council's written solicitation. The contractor must correct any and all defects in material and/or workmanship that may appear during the guarantee period, or any defects that occur within one (1) year of acceptance even if discovered more than one (1) year after acceptance, by repairing, (or replacing with new items or new materials, if necessary) any such defect at no cost to the County Council and to the County Council's satisfaction.

B. Should a manufacturer's or service provider's warranty or guarantee exceed the requirements stated above, that guarantee or warranty will be the primary one used in the case of defect. Copies of manufacturer's or service provider's warranties must be provided upon request.

C. All warranties and guarantees must be in effect from the date of acceptance by the County Council of the goods, services, or construction.

D. The contractor guarantees that all work shall be accomplished in a workmanlike manner, and the contractor must observe and comply with all Federal, State, County and local laws, ordinances and regulations in providing the goods, and performing the services or construction.

E. Goods and materials provided under this contract must be of first quality, latest model and of current manufacture, and must not be of such age or so deteriorated as to impair their usefulness or safety. Items that are used, rebuilt, or demonstrator models are unacceptable, unless specifically requested by the County Council in the Specifications.

14. HAZARDOUS AND TOXIC SUBSTANCES

Manufacturers and distributors are required by federal "Hazard Communication" provisions (29 CFR 1910.1200), and the Maryland "Access to Information About Hazardous and Toxic Substances" Law, to label each hazardous material or chemical container, and to provide Material Safety Data Sheets to the purchaser. The contractor must comply with these laws and must provide the County with copies of all relevant documents, including Material Safety Data Sheets, prior to performance of work or contemporaneous with delivery of goods.

15. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) COMPLIANCE

In addition to the provisions stated above in Section 3. "Applicable Laws," contractor must comply with all requirements in the federal Health Insurance Portability and Accountability Act (HIPAA), to the extent that HIPAA is applicable to this contract. Furthermore, contractor must enter into the County's standard Business Associate Agreement or Qualified Service Organization Agreement when contractor or the County, as part of this contract, may use or disclose to one another, to the individual whose health information is at issue, or to a third-party, any protected health information that is obtained from, provided to, made available to, or created by, or for, the contractor or the County.

16. IMMIGRATION REFORM AND CONTROL ACT

The contractor warrants that both the contractor and its subcontractors do not, and shall not, hire, recruit or refer for a fee, for employment under this contract or any subcontract, an alien while knowing the alien is an unauthorized alien, or any individual without complying with the requirements of the federal Immigration and Nationality laws, including any verification and record keeping requirements. The contractor further assures the County Council that, in accordance with those laws, it does not, and will not, discriminate against an individual with respect to hiring, recruitment, or

referral for a fee, of an individual for employment or the discharge of an individual from employment, because of the individual's national origin or, in the case of a citizen or prospective citizen, because of the individual's citizenship status.

17. INCONSISTENT PROVISIONS

Notwithstanding any provisions to the contrary in any contract terms or conditions supplied by the contractor, this General Conditions of Contract document supersedes the contractor's terms and conditions, in the event of any inconsistency.

18. INDEMNIFICATION

The contractor is responsible for any loss, personal injury, death and any other damage (including incidental and consequential) that may be done or suffered by reason of the contractor's negligence or failure to perform any contractual obligations. The contractor must indemnify and save the County harmless from any loss, cost, damage and other expenses, including attorney's fees and litigation expenses, suffered or incurred due to the contractor's negligence or failure to perform any of its contractual obligations. If requested by the County, the contractor must defend the County in any action or suit brought against the County arising out of the contractor's negligence, errors, acts or omissions under this contract. The negligence of any agent, subcontractor or employee of the contractor is deemed to be the negligence of the contractor. For the purposes of this paragraph, County includes its boards, agencies, agents, officials and employees.

19. INDEPENDENT CONTRACTOR

The contractor is an independent contractor. The contractor and the contractor's employees or agents are not agents of the County Council or the County.

20. INSPECTIONS

County Council representatives has the right to monitor, inspect and evaluate or test all supplies, goods, services, or construction called for by the contract at all reasonable places (including the contractor's place of business) and times (including the period of preparation or manufacture).

21. INSURANCE

Prior to contract execution by the County Council, the proposed awardee/contractor must obtain at its own cost and expense the insurance specified in the applicable table (See Tables A and B) or attachment to these General Conditions, with one or more insurance company(s) licensed or qualified to do business in the State of Maryland and acceptable to the County's Division of Risk Management. Contractor must keep this insurance in full force and effect during the term of this contract, including all extensions. Unless expressly provided otherwise, Table A is applicable to this contract. The insurance must be evidenced by one or more Certificate(s) of Insurance and, if requested by the County, the proposed awardee/contractor must provide a copy of any and all insurance policies to the County. At a minimum, the proposed awardee/contractor must submit to the Contract Administrator one or more Certificate(s) of Insurance prior to award of this contract, and prior to any contract modification extending the term of the contract, as evidence of compliance with this provision. The contractor's insurance must be primary. Montgomery County, MD, including its officials, employees, agents, boards, and agencies, must be named as an additional insured on all liability policies. Thirty days written notice to the County Council of cancellation or material change in any of the policies is required, unless a longer period is required by applicable law. In no event may the insurance coverage be less than that shown on the applicable table, attachment, or contract provision for required insurance. The Director, Office of Legislative Oversight, may waive the requirements of this section, in whole or in part.

RFP #425820958

TABLE A. - INSURANCE REQUIREMENTS
(See Paragraph #21 Under the General Conditions of Contract
Between County and Contractor)

CONTRACT DOLLAR VALUES (IN $1,000's)

	Up to 50	Up to 100	Up to 1,000	Over 1,000
Workers Compensation (for contractors with employees)				
Bodily Injury by				
Accident (each)	100	100	100	See Attachment
Disease (policy limits)	500	500	500	
Disease (each employee)	100	100	100	
Commercial General Liability minimum combined single limit for bodily injury and property damage per occurrence, including contractual liability, premises and operations, and independent contractors	300	500	1,000	See Attachment
Minimum Automobile Liability (including owned, hired and non-owned automobiles)				
Bodily Injury				
each person	100	250	500	See Attachment
each occurrence	300	500	1,000	
Property Damage Each occurrence	300	300	300	
Professional Liability* for errors, omissions and negligent acts, per claim and aggregate, with one year discovery period and maximum deductible of $25,000	250	500	1,000	See Attachment

Certificate Holder
Montgomery County Maryland (Contract #)
Office of Procurement
Rockville Center
255 Rockville Pike, Suite 180
Rockville, Maryland 20850-4166

*Professional services contracts only

(Remainder of Page Intentionally Left Blank)

RFP #425820958

TABLE B. - INSURANCE REQUIREMENTS
(See Paragraph #21 Under the General Conditions of Contract
Between County and Contractor)

	Up to 50	Up to 100	Up to 1,000	Over 1,000
Commercial General Liability minimum combined single limit for bodily injury and property damage per occurrence, including contractual liability, premises and operations, and independent contractors, and product liability	300	500	1,000	See Attachment

Certificate Holder
Montgomery County Maryland (Contract #)
Office of Procurement
Rockville Center
255 Rockville Pike, Suite 180
Rockville, Maryland 20850-4166

(Remainder of Page Intentionally Left Blank)

22. INTELLECTUAL PROPERTY APPROVAL AND INDEMNIFICATION - INFRINGEMENT

If contractor will be preparing, displaying, publicly performing, reproducing, or otherwise using, in any manner or form, any information, document, or material that is subject to a copyright, trademark, patent, or other property or privacy right, then contractor must: obtain all necessary licenses, authorizations, and approvals related to its use; include the County in any approval, authorization, or license related to its use; and indemnify and hold harmless the County related to contractor's alleged infringing or otherwise improper or unauthorized use. Accordingly, the contractor must protect, indemnify, and hold harmless the County from and against all liabilities, actions, damages, claims, demands, judgments, losses, costs, expenses, suits, or actions, and attorneys' fees and the costs of the defense of the County, in any suit, including appeals, based upon or arising out of any allegation of infringement, violation, unauthorized use, or conversion of any patent, copyright, trademark or trade name, license, proprietary right, or other related property or privacy interest in connection with, or as a result of, this contract or the performance by the contractor of any of its activities or obligations under this contract.

23. NON-CONVICTION OF BRIBERY

The contractor hereby declares and affirms that, to its best knowledge, none of its officers, directors, or partners or employees directly involved in obtaining contracts has been convicted of bribery, attempted bribery, or conspiracy to bribe under any federal, state, or local law.

24. NON-DISCRIMINATION IN EMPLOYMENT

The contractor agrees to comply with the non-discrimination in employment policies and/ or provisions prohibiting unlawful employment practices in County contracts as required by Section 11B-33 and Section 27-19 of the Montgomery County Code, as well as all other applicable state and federal laws and regulations regarding employment discrimination.

The contractor assures the County Council that, in accordance with applicable law, it does not, and agrees that it will not, discriminate in any manner on the basis of race, color, religious creed, ancestry, national origin, age, sex, marital status, disability, or sexual orientation.

The contractor must bind its subcontractors to the provisions of this section.

25. PAYMENTS

No payment by the County may be made, or is due, under this contract, unless funds for the payment have been appropriated and encumbered by the County Council. Under no circumstances will the County Council pay the contractor for legal fees. The contractor must not proceed to perform any work (provide goods, services, or construction) prior to receiving written confirmation that the County Council has appropriated and encumbered funds for that work. If the contractor fails to obtain this verification from the Contract Administrator prior to performing work, the County Council has no obligation to pay the contractor for the work.

If this contract provides for an additional contract term for contractor performance beyond its initial term, continuation of contractor's performance under this contract beyond the initial term is contingent upon, and subject to, the appropriation of funds and encumbrance of those appropriated funds for payments under this contract. If funds are not appropriated and encumbered to support continued contractor performance in a subsequent fiscal period, contractor's performance must end without further notice from, or cost to, the County Council or the County. The contractor acknowledges that the County Executive has no obligation to recommend, and the County Council has no obligation to appropriate, funds for this contract in subsequent fiscal years. Furthermore, the County Council has no obligation to encumber funds to this contract in subsequent fiscal years, even if appropriated funds may be available. Accordingly, for each subsequent contract term, the contractor must not undertake any performance under this contract until the contractor receives a purchase order or contract amendment from the Contract Administrator that authorizes the contractor to perform work for the next contract term.

The County is expressly permitted to pay the vendor for any or all goods, services, or construction under the contract through either a procurement card ("p-card") or a Single Use Account ("SUA") method of payment, if the contractor accepts the noted payment method from any other person. In that event, the County Council reserves the right to pay any or all amounts due under the contract by using either a p-card (except when a purchase order is required) or a SUA method of payment, and the contractor must accept the County's p-card or a SUA method of payment, as applicable. Under this paragraph, contractor is prohibited from charging or requiring the County Council to pay any fee, charge, price, or other obligation for any reason related to or associated with the County Council's use of either a p-card or a SUA method of payment.

26. PERSONAL PROPERTY

All furniture, office equipment, equipment, vehicles, and other similar types of personal property specified in the contract, and purchased with funds provided under the contract, become the property of the County Council upon the end of the contract term, or upon termination or expiration of this contract, unless expressly stated otherwise.

27. PROTECTION OF PERSONAL INFORMATION BY GOVERNMENT AGENCIES

In any contract under which Contractor is to perform services and the County Council or County may disclose to Contractor personal information about an individual, as defined by State law, Contractor must implement and maintain reasonable security procedures and practices that: (a) are appropriate to the nature of the personal information disclosed to the Contractor; and (b) are reasonably designed to help protect the personal information from unauthorized access, use, modification, disclosure, or destruction. Contractor's requirement to implement and maintain reasonable security practices and procedures must include requiring any third-party to whom it discloses personal information that was originally disclosed to Contractor by the County Council or the County to also implement and maintain reasonable security practices and procedures related to protecting the personal information. Contractor must notify the County and the Contract Administrator of a breach of the security of a system if the unauthorized acquisition of an individual's personal information has occurred or is reasonably likely to occur, and also must share with the County and the Contract Administrator all information related to the breach. Contractor must provide the above notification to the County as soon as reasonably practicable after Contractor discovers or is notified of the breach of the security of a system. Md. Code Ann., State Gov't. § 10-1301 through 10-1308 (2013).

28. TERMINATION FOR DEFAULT

The County Council may terminate the contract in whole or in part, and from time to time, whenever the County Council determines that the contractor is:

(a) defaulting in performance or is not complying with any provision of this contract;
(b) failing to make satisfactory progress in the prosecution of the contract; or
(c) endangering the performance of this contract.

The County Council will provide the contractor with a written notice to cure the default. The termination for default is effective on the date specified in the County Council's written notice. However, if the County Council determines that default contributes to the curtailment of an essential service or poses an immediate threat to life, health, or property, the County Council may terminate the contract immediately upon issuing oral or written notice to the contractor without any prior notice or opportunity to cure. In addition to any other remedies provided by law or the contract, the contractor must compensate the County Council for additional costs that foreseeably would be incurred by the County Council whether the costs are actually incurred or not, to obtain substitute performance. A termination for default is a termination for convenience if the termination for default is later found to be without justification.

29. TERMINATION FOR CONVENIENCE

This contract may be terminated by the County Council, in whole or in part, upon written notice to the contractor, when the County Council determines this to be in its best interest. The termination for convenience is effective on the date specified in the County Council's written notice. Termination for convenience may entitle the contractor to payment for reasonable costs allocable to the contract for work or costs incurred by the contractor up to the date of termination. The contractor must not be paid compensation as a result of a termination for convenience that exceeds the amount encumbered to pay for work to be performed under the contract.

30. TIME

Time is of the essence.

31. WORK UNDER THE CONTRACT

Contractor must not commence work under this contract until all conditions for commencement are met, including execution of the contract by both parties, compliance with insurance requirements, encumbrance of funds, and issuance of any required notice to proceed.

32. WORKPLACE SAFETY

The contractor must ensure adequate health and safety training and/or certification, and must comply with applicable federal, state and local Occupational Safety and Health laws and regulations.

END SECTION B - GENERAL CONDITIONS OF CONTRACT BETWEEN COUNTY COUNCIL AND CONTRACTOR

SECTION C - SCOPE OF SERVICES

BACKGROUND

Introduction. Montgomery County, Maryland is the most populated and affluent jurisdiction in the State of Maryland. The County contains 497 square miles and approximately 1,017,000 people. In the fall of 2014, 153,852 pupils were enrolled in the County's schools. The median household income (in 2013) was $98,326. In September 2014, the County's labor force totaled approximately 529,000, with an unemployment rate of 4.5%.

The Charter, the governing authority of the County, provides for separate legislative and executive branches of government. Legislative power is vested in an elected County Council and executive power in an elected County Executive. Under the County Charter, the County Executive develops and recommends budget proposals and the Council authorizes expenditures and sets property tax rates. It is the fiscal policy of Montgomery County to balance the budget, such that no deficit is planned or incurred.

The Charter provides for an annual six-year Public Services Program, Operating Budget, Capital Budget, and biennial six-year Capital Improvements Program (CIP). These budgets and plans provide the basis for understanding, coordinating, and controlling County government expenditures and programs. County Government program areas include:

- Education,
- Public safety,
- Public works and transportation,
- Culture and recreation,
- Health and human services,
- Community development and housing,
- Environment, and
- General government services.

Financial Reporting. For financial reporting purposes, the County's reporting entity consists of: (1) the primary government, and (2) component unit organizations, including:

- Montgomery County Public Schools,
- Montgomery Community College,
- Housing Opportunities Commission of Montgomery County,
- Montgomery County Revenue Authority, and
- Bethesda Urban Partnership, Inc.

Additionally, the following organizations are included in the Montgomery County, Maryland reporting entity as joint ventures:

- Montgomery County's portion of the Maryland-National Capital Park and Planning Commission,
- Washington Suburban Sanitary Commission,
- Washington Suburban Transit Commission,
- Washington Metropolitan Area Transit Authority,
- Metropolitan Washington Council of Governments, and
- Northeast Maryland Waste Disposal Authority.

SECTION C - SCOPE OF SERVICES (continued**)**

Montgomery County's basic financial statements include three components: government-wide financial statements, fund financial statements, and notes to the financial statements. The focus in the fund financial statements is on the major funds, with major funds reported separately and all other funds combined into a single, aggregated presentation. The County has the following three types of funds:

- **Governmental Funds** – Most of the County's basic services are included in Governmental Funds. The three major governmental funds are the General Fund, Debt Service Fund, and Capital Projects Fund.

- **Proprietary Funds** – Proprietary Funds consist of enterprise funds and internal service funds. The County has three major enterprise funds, including liquor control, solid waste disposal and collection, and parking lot districts. The internal service funds account for the provision of liability and property insurance coverage, employee health benefits, motor pool services, and central duplicating services.

- **Fiduciary Funds** – Fiduciary Funds are used to account for resources held for the benefit of parties outside the government. They consist of pension and other employee benefit trusts, an investment trust, private purpose trusts, and agency funds.

The County prepares and presents its Comprehensive Annual Financial Report (CAFR) consistent with Generally Accepted Accounting Principles for governments, as set forth by the Governmental Accounting Standards Board (GASB). Montgomery County, Maryland has received the Government Finance Officers Association's (GFOA) Certificate of Achievement for Excellence in Financial Reporting 45 times, more than any other county in the nation.

The County also manages and accounts for its Operating and Capital Budgets in accordance with Generally Accepted Accounting Principles. Montgomery County has received the GFOA Distinguished Budget Presentation award consecutively since 1984, the year the program was established.

Pension and Deferred Compensation Benefits. The County sponsors two cost-sharing multiple-employer pension plans, in which other agencies and political subdivisions have the right to elect participation. The County prepares a separate Comprehensive Annual Financial Report (CAFR) for the Montgomery County Employee Retirement Plans.

The Employees' Retirement System of Montgomery County is a defined benefit pension plan. The plan is closed to employees hired on or after October 1, 1994 (except public safety bargaining unit employees). The Guaranteed Retirement Income Plan, a cash balance plan option, covers non-public safety and certain public safety (non-bargaining unit) employees hired on or after October 1, 1994 who elect to participate. The plan's assets are exclusively managed by the Board of Investment Trustees, which consists of thirteen trustees and functions as part of the County. The annual contribution required for this plan is based on an actuarial valuation.

The Employees' Retirement Savings Plan, a defined contribution plan, also covers non-public safety and certain public safety (non-bargaining unit) employees hired on or after October 1, 1994 who elect to participate. The Board of Investment Trustees selects a slate of investment options for participating employees in the RSP.

All component unit organizations participate in various pension plans, either directly in their own plan or through participation in pension systems of Montgomery County or the State of Maryland. The Housing Opportunities Commission and Montgomery County Revenue Authority participate in the Employees' Retirement System or Employees' Retirement Savings Plan of Montgomery County.

The County sponsors the Montgomery County Deferred Compensation Plan pursuant to Section 457 of the Internal Revenue Code. The assets are held in trust for the sole benefit of participants and their beneficiaries. Trust responsibilities are assigned to the Board of Investment Trustees.

SECTION C - SCOPE OF SERVICES (continued)

INTENT

The intent of this solicitation is to procure professional auditing services, including:

Independent audit of the basic financial statements of Montgomery County and independent audit of the basic financial statements of the Montgomery County Employee Retirement Plans, and preparation of and independent audit of the basic financial statements of the Montgomery County Union Employees Deferred Compensation Plan, and additional services related to reviews, tests, and certifications.

WORK STATEMENT

a) **Basic Financial Statements Audit** – The Contractor must audit the financial statements of the governmental activities, the business-type activities, the aggregate discretely presented component units, each major fund, and the aggregate remaining fund information of Montgomery County. The Contractor must prepare an Independent Auditors' Report to express opinions on the basic financial statements. The Contractor's opinion may place reliance on reports issued by other Contractors as they relate to component units. The Contractor must also provide a training on new and/or updated auditing standards at the Department of Finance's annual Year-End Component Unit Planning Meeting.

b) **Single Audit** – As required by Federal OMB Uniform Guidance, the Contractor must 1) examine the Montgomery County Report on Expenditures of Federal Awards, 2) complete the auditor's portion of the Uniform Guidance data collection form, and 3) review internal accounting and administrative controls. The Contractor must prepare Independent Auditors' Reports on:

- Compliance and Internal Control Over Financial Reporting Based on an Audit of Financial Statements in Accordance with Government Auditing Standards,
- Compliance with Requirements Applicable to Each Major Program, Internal Control Over Compliance, and Schedule of Expenditures of Federal Awards in Accordance with OMB Circular A-133,
- Status of prior year findings and questioned costs, and
- Schedule of findings and questioned costs.

c) **Agreed-Upon Procedures for the Chief Financial Officer's Annual Certification of Financial Assurance Mechanisms for Local Government Owners and Operators of Municipal Solid Waste Landfill Facilities** – To comply with Environmental Protection Agency requirements, the Contractor must review and perform agreed-upon procedures to the Chief Financial Officer's Annual Certification of Financial Assurance Mechanisms for Local Government Owners and Operators of Municipal Solid Waste Landfill Facilities. The Contractor must prepare an Independent Auditors' Report on Applying Agreed-Upon Procedures.

d) **Maryland State Uniform Financial Report** – The Contractor must review and attest to the County's uniform financial report submitted to the Maryland State Division of Fiscal Services, and transmit completed forms as required.

e) **Management Letter** – The Contractor must prepare a management letter to submit to the County Council at the completion of the annual audit of the basic financial statements of the County. The Contractor must include comments, recommendations, and suggested improvements in accounting procedures, internal controls, management actions, and other relevant areas.

SECTION C - SCOPE OF SERVICES (continued)

f) **Government Finance Officers Association (GFOA) Certificate of Achievement for Excellence in Financial Reporting** – The Contractor must assist the County to ensure that the County's Comprehensive Annual Financial Report (CAFR) complies with the GFOA standards for the Certificate of Achievement. The specific standards require financial disclosure greater than is required under generally accepted accounting principles.

g) **Fiscal Year Closing** – The Contractor must participate in the annual planning meeting with the component units included in the Montgomery County, Maryland reporting entity. The annual planning meeting involves discussing the fiscal year closing process and identifying any issues that may impact the timing of the closing. The Contractor must specifically discuss any mandated or proposed reporting changes that would apply to the current fiscal year and subsequent fiscal years.

Note: A separate price sheet is required for items a) through g) listed above. See Attachment page F1.

h) **Agreed-Upon Procedures for the National Transit Database (NTD) Report** – The Contractor must apply agreed-upon procedures to the National Transit Database Report prepared by Montgomery County to assist the County to evaluate whether the information included in the Federal Funding Allocation Statistics Form conforms with Federal Transit Administration requirements. The Contractor must prepare an Independent Auditors' Report on applying agreed-upon procedures to the NTD Report's Federal Funding Allocation Statistics Form. Note: A separate price sheet is required for this activity. See Attachment page F2.

i) **9-1-1 System Audit** – The Contractor must conduct an audit of the Schedule of Revenues and Expenditures of the County's 9-1-1 System. The Contractor must submit a Schedule of Revenues and Expenditures. The Contractor must prepare an Independent Auditors' Report to express opinions on the Schedule of Revenues and Expenditures. Note: A separate price sheet is required for this activity. See Attachment page F3.

j) **Optional Work** – The County Council, acting through the Audit Committee, may select areas for special attention by the Contractors. Additionally, the County's Department of Finance may request consulting services on specific financial or internal control reporting requirements. As required, the County Council will amend the contract to include optional work. Optional work may include:

- Auditing Services – The County may require additional audits or audit related services, including IT-related services. These professional services shall be delivered only upon specific authorization of the Contract Administrator, as evidenced by the issuance of a notice-to-proceed.

- Accounting Services – The County may require professional accounting services and/or IT-related services from the Contractor to 1) assist with the close of the County's books, 2) assist with preparation of draft schedules to support each fund and draft financial statements, and 3) provide other related professional services. These services shall be delivered only upon specific authorization of the Contract Administrator, as evidenced by the issuance of a notice-to-proceed.

- Comfort or Consent Letters – The County may require that the Contractor perform tests and analyses, in accordance with generally accepted auditing standards, to issue a comfort or consent letter authorizing the County to use the Auditors' opinion in County debt offering documents. These services shall be delivered only upon specific authorization of the County's Director of Finance, as evidenced by the issuance of a notice-to-proceed.

SECTION C - SCOPE OF SERVICES (continued)

- Arbitrage – The Contractor will review and report on the calculation of rebate amount under the U.S. Treasury arbitrage rebate requirements (if applicable).

Note: A separate price sheet is required for the optional work listed above. See Attachment page F4.

k) **Employee Retirement Plans Financial Statements Audit** – The Contractor must audit the Comprehensive Annual Financial Report of the County Employee Retirement Plans in sufficient detail to render an opinion that the financial statements present fairly in all material respects, the financial position of the retirement funds. The Contractor will be responsible for performing all testing and other related procedures as recommended by the AICPA State and Local Government Expert Panel White Paper entitled "Governmental Employer Participation in Cost- Sharing Multiple-Employer Plans: Issues Related to Information for Employer Reporting" as well as other applicable guidance to the extent the Plans and the County has prepared the recommended schedules and other information included in this guidance. The Contractor must prepare an Independent Auditors' Report to express opinions on the financial statements.

l) **Other Post-Employment Benefits** – The County's Retiree Health Benefits Trust accumulates resources needed for the County's primary post-employment benefit—health insurance. While the trust is part of the County's basic financial statements, the Plan is a cost-sharing multiple-employer one. As such, several agencies participate in the Plan. The Contractor will be responsible for performing all testing and other related procedures as recommended by the AICPA related to GASB Statement numbers 74 and 75.

m) **Management Letter** – The Contractor must prepare a management letter to submit to the County Council at the completion of the annual audit of the financial statements of the Retirement Plans. The Contractor must include comments, recommendations, and suggested improvements in accounting procedures, internal controls, management actions, and other relevant areas.

n) **Government Finance Officers Association (GFOA) Certificate of Achievement for Excellence in Financial Reporting** – The Contractor must assist the County to ensure that the Employee Retirement Plans' Comprehensive Annual Financial Report (CAFR) complies with the GFOA standards for the Certificate of Achievement. The specific standards require financial disclosure greater than required under generally accepted accounting principles.

Note: A separate price sheet is required for items k) through n). See Attachment page F5.

o) **Montgomery County Union Employees Deferred Compensation Plan Basic Financial Statements Audit** – The Contractor must prepare the annual financial statements for and audit the financial statements of the Montgomery County Union Employees Deferred Compensation Plan for calendar year 2016. The audit must be performed in accordance with *Government Auditing Standards*. The Contractor must prepare:

- Annual financial statements for the Montgomery County Union Employees Deferred Compensation Plan,
- An Independent Auditors' Report to express opinions on whether the financial statements fairly present, in all material respects, the financial position of the deferred compensation plan, and
- An Independent Auditors' Report on Compliance and Internal Control Over Financial Reporting Based on an Audit of Financial Statements in Accordance with *Government Auditing Standards*.

Note: A separate price sheet is required for item o). See Attachment page F6.

SECTION C - SCOPE OF SERVICES (continued)

DELIVERABLES

The Contractor must provide **up to 20 hard copies and an electronic copy** of the following deliverables to be incorporated into the County's CAFR **in time for submission for the Government Finance Officers Association (GFOA) Certificate of Achievement for Excellence in Financial Reporting program**:

a) Independent Auditors' Report to express opinions on the basic financial statements of the County Government, and

b) Independent Auditors' Report to express opinions on the basic financial statements of the Montgomery County Employee Retirement Plans.

The Contractor must provide **up to 20 hard copies and an electronic copy** of the following deliverables **by December 15th** of each year that a contract resulting from this RFP remains in place (see Section D – Performance Period)**,** unless the Contractor and County mutually agree on an alternative date:

c) Independent Auditors' Report on Compliance and Internal Control Over Financial Reporting Based on an Audit of Financial Statements in Accordance with Government Auditing Standards (Single Audit),

d) Independent Auditors' Report on Compliance with Requirements Applicable to Each Major Program, Internal Control Over Compliance, and Schedule of Expenditures of Federal Awards in Accordance with OMB Uniform Guidance (Single Audit),

e) Independent Auditors' Report on the status of prior year findings and questioned costs (Single Audit),

f) Independent Auditors' Report on the schedule of findings and questioned costs (Single Audit),

g) Auditor's portion of the Single Audit Act data collection form (Single Audit),

h) Independent Auditors' Report on Applying Agreed-Upon Procedures to the Chief Financial Officer's Annual Certification of Financial Assurance Mechanisms for Local Government Owners and Operators of Municipal Solid Waste Landfill Facilities,

i) Auditor signature page of the Maryland State Uniform Financial Report,

j) Report on the calculation of rebate amount under the U.S. Treasury arbitrage rebate requirements (if applicable),

k) Independent Auditors' Report on Applying Agreed-Upon Procedures to the Federal Funding Allocation Statistics Form of the National Transit Database Report,

l) Independent Auditors' Report to express opinions on the Schedule of Revenues and Expenditures of the County's 9-1-1 System, and

m) Schedule of Revenues and Expenditures for the County's 9-1-1 System.

The Contractor must provide **up to 20 hard copies and an electronic copy** of the following deliverables **by March 1st** of each year that a contract resulting from this RFP remains in place (see Section D – Performance Period):

n) Management Letter related to the audit of the financial statements of Montgomery County, and

o) Management Letter related to the audit of the financial statements of the Montgomery County Employee Retirement Plans.

The Contractor must provide **up to 20 hard copies and an electronic copy** of the following deliverables **by June 1st** of each year that a contract resulting from this RFP remains in place (see Section D – Performance Period):

SECTION C – SCOPE OF SERVICES (continued)

p) Annual financial statements for the Montgomery County Union Employees Deferred Compensation Plan

q) Independent Auditors' Report to express opinions on the basic financial statements of the Montgomery County Union Employees Deferred Compensation Plan, and

r) Independent Auditors' Report on Compliance and Internal Control Over Financial Reporting of the Montgomery County Union Employees Deferred Compensation Plan Based on an Audit of the Financial Statements in Accordance with *Government Auditing Standards*.

s) Management Letter related to the audit of the financial statements of the Montgomery County Union Employees Deferred Compensation Plan.

Additional required deliverables include:

t) A presentation to the Council's Audit Committee to review the Contractor's reports and Management Letters, and

u) Written monthly reports to the Contract Administrator summarizing progress to date and any accounting or auditing concerns that may impact items in the Work Statement.

OFFEROR QUALIFICATIONS

The Offeror must:

- Be a licensed certified public accounting firm,
- Be a firm with experience in auditing local governments similar to Montgomery County and experience conducting audits that meet Government Auditing Standards (2007 Revision),
- Have staff members with experience auditing local governments similar to Montgomery County and experience conducting audits that meet Government Auditing Standards (2007 Revision),
- Be in compliance with provisions of the Business Occupations & Professions Article, Title 2, of the Annotated Code of Maryland, which govern the practice of public accounting within the State of Maryland,
- Meet the independence requirements of Government Auditing Standards, published by the Comptroller General of the United States,
- Have experience auditing large local governments similar to Montgomery County that have implemented Government Accounting Standards Board (GASB) Statement No. 34, and
- Have the capacity to audit computerized systems and knowledge of computer assisted audit techniques.

SECTION C – SCOPE OF SERVICES (continued)

CONTRACTOR RESPONSIBILITY

The Contractor is responsible for completing the work described in Section C – Scope of Services of this RFP to the Council's satisfaction. Additional Contractor responsibilities include:

1. ACCOUNTING AND AUDITING STANDARDS

The Contractor must conduct the audits in accordance with the following accounting and auditing standards, as applicable:

1. Governmental Accounting Standards Board (GASB) Codification of Governmental Accounting and Financial Reporting Standards, and other GASB publications,
2. Generally accepted auditing standards prescribed by the American Institute of Certified Public Accountants, including the industry audit guides for "Audits of State and Local Governmental Units,"
3. Government Auditing Standards, Comptroller General of the United States,
4. OMB Uniform Guidance and Related Compliance Supplements
5. Audit Guidelines prescribed by the Legislative Auditor of the State of Maryland,
6. Audit Guidelines for examination of 9-1-1 Trust Funds, as prescribed by the Emergency Number Systems Board of the Maryland Department of Public Safety and Correctional Services,
7. Examination Guidelines and Certification Requirements prescribed by the Urban Mass Transit Transportation Administration,
8. Federal Information System Controls Auditing Manual, if applicable,
9. Consideration of Fraud in a Financial Statement Audit (Statement on Auditing Standards #99), and
10. Other professional auditing/accounting standards issued, as appropriate.

2. COUNTY'S ACCOUNTING SYSTEM AND RECORDS

Montgomery County has an on-line computerized accounting and financial reporting system, Oracle eBusiness Suite (EBS), which will be made available to the Contractor under the requirements of and restrictions in Administrative Procedure 6-1, Use of County-Provided Internet, Intranet, and E-Mail Services and in Administrative Procedure 6-7, Information Resources Security. Attached at Appendix H. The Contractor's techniques and procedures must be modified, if necessary, to be used with the County's existing systems. The Contractor must utilize the on-line nature of the accounting system to the fullest extent possible.

3. ACCESS TO COUNTY RECORDS AND STAFF

The Contractor will have access to County records and staff for the purposes of interviews and verification of items within the terms of the audit. The Contractor must maintain such records as privileged and confidential information. If granted either physical or data rights, the Contractor must only access those items necessary to perform the audit.

The Contractor must organize the work in such a way as to minimize disruption of work of County employees in the pursuit of their normal duties. The Contractor must provide the County at least 3 full business days to prepare written or oral responses to Contractor requests for information.

4. CONFIDENTIAL INFORMATION

Some material to be reviewed by the Contractor in performance of a contract will be of a confidential or proprietary nature. The Contractor must not divulge such confidential or proprietary information to any party other than the authorized officers of the local fire and rescue departments, the County Council, or other County officials directly involved.

SECTION C – SCOPE OF SERVICES (continued)

5. CONTRACTOR STAFF

Key personnel (partner, managers, supervisors, and seniors) of the Contractor's staff must work at the level of effort proposed by the Contractor unless a change is authorized by the Office of Legislative Oversight. The Contractor must notify the Contract Administrator in writing if it becomes necessary to replace any of the key personnel. The Contractor must provide the resumes for new personnel assigned to the work, and the new personnel's qualifications and experience must be at least equal to those of the replaced staff. The Contract Administrator must approve the personnel change in writing prior to the change taking place.

6. VERIFICATION AND AUDITS

The Contractor and all subcontractors must maintain for a period of five years, books, records, documents, and other evidence directly pertinent to the performance of work under this contract ("audit documentation"), in accordance with appropriate accounting procedures and generally accepted government auditing standards. The Contractor must make audit documentation available, upon written request, in a timely manner to other auditors or reviewers in accordance with generally accepted government auditing standards. At the County's request, the Contractor must provide proper facilities within its offices during normal business hours, for purposes of making audit documentation available to such other auditors or reviewers.

COUNTY RESPONSIBILITY

1. PRE-SUBMISSION CONFERENCE

The Office of Legislative Oversight will conduct a pre-submission conference at **2:00 p.m. on Thursday, September 10, 2015 in the 6th Floor Conference Room of the Council Office Building, 100 Maryland Avenue, Rockville, MD 20850**. The following representatives will be present to respond to questions and discuss the County's financial structure and computer operations:

- County Finance Director or designee,
- Department of Finance staff,
- Montgomery County Employee Retirement Plans staff,
- Department of Technology Services staff,
- Other County representatives, and
- Other representatives, as necessary.

2. ACCESS TO COUNTY RECORDS AND STAFF

The County must provide the Contractor access to County records and reasonable access to the County staff for purposes of interviews and verification of items within the terms of the audit.

3. DEPARTMENT OF FINANCE SUPPORT

The County must provide limited, temporary space to examine records and documents during the audit, and must provide the capability to view on-line documents. The Department of Finance must also provide the following clerical and technical support to the Contractor:

- Type confirmation requests and other correspondence requesting information from government agencies,
- Retrieve and replace source documents located in the Department; however, on-line documents should be used to the fullest extent possible,
- Draft the financial statements, both in the preliminary and final forms,
- Type and reproduce the annual report, and
- Prepare a closing schedule that highlights the relevant activities and availability dates for workpapers and reports.

SECTION C – SCOPE OF SERVICES (continued)

4. DEPARTMENT OF TRANSPORTATION SUPPORT

The Department of Transportation must:

- Prepare the National Transit Database Report, Federal Funding Allocation Statistics Form,
- Prepare the passenger mile data collection calculation,
- Provide access to general ledger reports, and
- Provide access to vendor contracts and monthly Contractor reports.

5. DEPARTMENT OF TECHNOLOGY SERVICES SUPPORT

The Department of Technology Services must:

- Provide access to appropriate staff for interviews,
- Supply listings, reports, policies, and logs as required to support the audit,
- Generate limited rights audit user IDs for use within the local network, and
- Coordinate all responses for Information Technology requests.

The Department of Technology Services can only provide support for audit work related to organizations under the Department of Technology Services' management.

MONTGOMERY COUNTY UNION EMPLOYEES DEFERRED COMPENSATION PLAN RESPONSIBILITY

The Montgomery County Union Employees Deferred Compensation Plan (MCUEDCP) must provide access to its records and reasonable access to its staff for the purposes of interviews and verification of items within the terms of the audit. The MCUEDCP must facilitate the provision of its records and data from its plan administrator to the auditor. The MCUEDCP must provide limited, temporary space to examine records and documents during the audit and must also provide the following clerical and technical support to the Contractor:

- Type confirmation requests and other correspondence requesting information from the County Government, banks, attorneys, government agencies, and other entities as needed by the Contractor, and
- Retrieve and replace source documents in the possession of the MCUEDCP.

END SECTION C - SCOPE OF SERVICES

SECTION D - PERFORMANCE PERIOD

1. TERM

The term of the contract is for one year from the date of signature by the President of the County Council. The first engagement period will be from July 1, 2016 to June 30, 2017. The audit-year for the first engagement period will be July 1, 2015 through June 30, 2016 or Fiscal Year 2016 for Work Statement Parts a) through n) and will be January 1, 2016 through December 31, 2016 or Calendar Year 2016 for Work Statement Part o). Before the contract term ends, the County Council may (but is not required to) renew this contract, if the Council determines that renewal is in the best interest of the County. Contractor's satisfactory performance does not guarantee renewal of this Contract. The Council may exercise this option to renew for three additional one year periods, specifically for audits of fiscal years ending on June 30, 2017, 2018, and 2019 and for calendar years ending on December 31, 2017, 2018, and 2019.

2. PRICE ADJUSTMENTS

Prices quoted are firm for a period of two years after execution of the contract. Any request for a price adjustment, after this two-year period is subject to the following:

- Approval or rejection by the County Council;
- Submitted in writing to the Contract Administrator, Office of Legislative Oversight and accompanied by supporting documentation justifying the Contractor's request. A request for any price adjustment may not be approved unless the Contractor submits to the County Council sufficient justification to support that the Contractor's request is based on its net increase in costs in delivering the goods/services under the contract;
- Submitted sixty (60) days prior to the contract expiration date, if the contract is being amended;
- May not be approved which exceeds the amount of the annual percentage change of the Consumer Price Index (CPI) for the twelve-month period immediately prior to the date of the request. The request shall be based upon the CPI for all urban consumers issued for the Washington-Baltimore, DC-MD-VA-WV Metropolitan area by the United States Department of Labor, Bureau of Labor Statistics for all items;
- The Council will approve only one price adjustment for each contract term, if a price adjustment is approved;
- Should be effective sixty (60) days from the date of receipt of the Contractor's request; and
- Executed by written contract amendment.

END OF SECTION D - PERFORMANCE PERIOD

SECTION E - METHOD OF AWARD/EVALUATION CRITERIA

1. PROCEDURES
   a. Upon receipt of proposals, a Selection Committee will review and evaluate all proposals in accordance with the evaluation criteria listed in Section E.2.a.
   b. The Selection Committee will investigate Offerors to determine responsibility.
   c. The County Council's Audit Committee, or their designees, will conduct interviews with the three highest scoring Offerors based on the combined scores of the Selection Committee members' written proposal evaluations. The interview criteria are listed in Section E.2.b.
   d. The Audit Committee will recommend award of the highest ranked Offeror to the County Council, based on the combined scores of the Selection Committee members' written proposal evaluations, interview evaluations, and responsibility determination by the Selection Committee.
   e. The County Council will approve or reject the Audit Committee's recommendation.
   f. The Office of Legislative Oversight will then enter into contract negotiations with the approved top-ranked Offeror(s), with the negotiated contract subject to County Council approval.
   g. If a contract cannot be successfully negotiated with the top-ranked Offeror(s), the Office of Legislative Oversight may proceed to negotiate with the next highest ranked Offeror(s). **The Council reserves the right to cancel the solicitation.**

2. EVALUATION CRITERIA

a. Written Proposal Evaluation Criteria

The Selection Committee will evaluate the written proposals based on the following criteria:	Points
1. The Offeror's experience in auditing local governments, including grants. The Offeror's experience in auditing local governments similar to Montgomery County, Maryland. The Offeror's experience auditing local governments that have implemented GASB Statement No. 34 (if applicable). The capability of the Offeror's local office to support the engagement. The Offeror's quality control procedures.	25
2. The qualifications and experience of the Offeror's staff assigned to the audit, including subcontractors and contracted employees. The education of the staff assigned to the audit, including continuing professional education in governmental accounting and auditing. The years of experience of staff in auditing local government programs, activities, and grants.	25
3. The comprehensiveness of the audit work plan. The time estimates for each major segment of the work plan and estimated number of hours for each staff level assigned.	25
4. The responsiveness of the proposal in clearly explaining the Offeror's understanding of the Scope of Services.	15
5. Cost	10
Highest possible written proposal evaluation score per rater:	**100**

SECTION E - METHOD OF AWARD/EVALUATION CRITERIA (continued)

b. Interview Evaluation Criteria

The Audit Committee will evaluate the interviews based on the following criteria:	Points
1. The Offeror's experience in auditing local governments, including grants. The Offeror's experience auditing local governments similar to Montgomery County, Maryland. The Offeror's experience auditing local governments that have implemented GASB Statement No. 34 (if applicable).	25
2. The qualifications and experience of the Offeror's staff assigned to the audit, including subcontractors and contracted employees. The Offeror's commitment to ensuring continuity of the partner, manager, and senior accountant assigned to the engagement.	25
3. The Offeror's a) understanding of the Scope of Services, b) presentation of the audit work plans, and c) understanding of the deliverables.	25
4. The Offeror's ability to effectively communicate orally.	15
5. Cost.	10
Highest possible interview evaluation score per rater:	**100**

END OF SECTION E - METHOD OF AWARD/EVALUATION CRITERIA

SECTION F – PROPOSAL SUBMISSIONS

FAILURE OF AN OFFEROR TO SUBMIT ALL REQUIRED PROPOSAL SUBMISSIONS MAY RENDER YOUR PROPOSAL UNACCEPTABLE AS DETERMINED BY THE DIRECTOR, OFFICE OF LEGISLATIVE OVERSIGHT.

Offerors must submit **one original and seven (7) copies** of their proposal in the format described below. Written proposals will be evaluated on only what is submitted. The Offeror must submit sufficient information to enable the Selection Committee, Audit Committee, and County Council to evaluate the Offeror's capabilities and experience.

Proposals must include the following information in labeled sections:

1. A **Cover Letter** with a brief description of the firm, including the Offeror's name, address, telephone number, e-mail address, and fax number. The cover letter should also include brief statements showing the firms understanding of the auditing services to be performed.

2. The **Acknowledgment Page** (see page 5 of the RFP) of this solicitation must be submitted and signed by a person authorized to bind the Offeror to the proposal.

3. A **Profile of the Firm** that describes:

   - Firm's qualifications and experience in auditing local governments and grants, as well as local governments comparable to Montgomery County, Maryland. Specific experience in matters particular to Montgomery County (e.g., using the Oracle eBusiness Suite),
   - Firm's experience auditing local governments that have implemented GASB Statement No. 34 (if applicable),
   - Staff assigned to the audit, including resumes identifying relevant experience and the number of hours of continuing professional education in governmental accounting and auditing,
   - Capability to audit computerized systems, evaluate the efficient and effective use of on-line computer systems, and offer suggestions for improvement,
   - Extent to which computer-assisted audit techniques are relied upon,
   - Quality control procedures and measures to ensure a high quality audit,
   - All contracts the Offeror is currently performing or has performed for Montgomery County in the last five years, including all component units,
   - Any pending law suits or claims against the firm that the County Council should be aware of, and the nature of the law suits and claims, and
   - The results of the firm's latest external quality review.

4. An explanation of the firm's **Current Workload**, including the capacity of the local office to comply with the requirements of the first engagement period and potential subsequent engagement periods, including ensuring continuity of the partner, manager, and other senior staff. **Proposals submitted as part of the selection process must explain how the auditor intends to use auditing industry standards and best management practices to ensure auditor independence throughout the course of an engagement. In particular, incumbent auditors must demonstrate how, if selected, the firm's continuation as auditor is preferable to the Council's previous policy requiring auditor rotation after eight years**.

SECTION F – PROPOSAL SUBMISSIONS (continued)

5. A description of the firm's **Technical Approach** to completing the work described in Section C – Scope of Services, Work Statement and Section C – Scope of Services, Deliverables. The Technical Approach section of the proposal must include:

   - A detailed description of the auditing services that the firm will provide,
   - The specific work plans, including time estimates for each significant segment of the work, a scheduling plan, and the number of hours allocated by staff level (e.g., partner, manager, seniors, staff accountants),
   - A description of how the Offeror expects to use County staff to facilitate the work,
   - A description of the Offeror's computer assisted auditing techniques and analytical software tools to be used,
   - An explanation of the Offeror's expected use of the County's on-line accounting systems and system downloads to perform the audit work,
   - An explanation of the Offeror's approach to auditing electronic data processing/information technology procedures and controls,
   - An explanation of the Offeror's expected reliance on internal controls in lieu of performing substantive procedures,
   - Policies and practices on participating in entrance and exit conferences, issuing reports and Management Letters, communicating weaknesses noted in the accounting and internal control systems, and following-up on weaknesses and deficiencies noted, and
   - Discussion of potential problems or concerns associated with the Scope of Services, and recommended methods of addressing and resolving the potential problems or concerns.

6. A discussion of the use, if any, of **Subcontractors**. Firms submitting proposals that include subcontractors must identify the:

   - Proposed responsibilities of each subcontractor,
   - Each subcontractor's experience auditing local governments like Montgomery County,
   - Experience of each subcontractor's staff in auditing local governments, and the number of the subcontractor staffs' hours of continuing professional education in governmental accounting and auditing, and
   - The Offeror's pervious experiences in working with the subcontractors.

   The firm should not plan to use subcontractors to perform any audit segment in its entirety.

7. At least three **References** of current and/or previous government clients from three different jurisdictions who may be contacted to attest to the quality and timeliness of the Offeror's work of similar nature and scope to that required by the County Council. (see Attachment A)

8. The firm must submit the **Wage Requirements forms** in Attachment E. **Failure to submit the required material information in Attachment F will make your proposal unacceptable and it will be rejected.**

SECTION F – PROPOSAL SUBMISSIONS (continued)

9. **Price Sheets** that separately designate the firm fixed price for specific portions of the work described in Section C – Scope of Services, Work Statement, for the engagement period beginning July 1, 2016 and ending June 30, 2017. The price sheets must be submitted in the formats found in Attachment F, with separate sheets for the segments of work described below.

   Price sheets for the audit of the County's financial statements and additional services related to reviews, tests, and certifications must include:

   - A firm fixed price for the work described in parts a) through g) of the Work Statement (see page 24-25). It must incorporate the cost for up to 20 copies of all reports and management letters to be submitted. The price sheet must be submitted in the format attached at page F1.
   - A firm fixed price for the work described in part h) of the Work Statement (see page 25). It must incorporate the cost for up to 20 copies of all reports. The price sheet must be submitted in the format attached at page F2.
   - A firm fixed price for the work described in part i) of the Work Statement (see page 25). It must incorporate the cost of up to 20 copies of all reports and schedules. The price sheet must be submitted in the format attached at page F3.
   - A firm fixed price for the work described in part j) Auditing Services of the Work Statement (see page 25). It must present a fixed hourly rate for Auditing Services and be submitted in the format attached at page F4.
   - A firm fixed price for the work described in part j) Accounting Services of the Work Statement (see page 25). It must present a fixed hourly rate for Accounting Services and be submitted in the format attached at page F4.
   - A firm fixed price for the work described in part j) Comfort or Consent Letters of the Work Statement (see page 25). It must present a fixed fee for each letter. It must be submitted in the format attached at page F4.

   Price sheets for the audit of the Employee Retirement Plans must include:

   - A firm fixed price for the work described in parts k) through n) of the Work Statement (see page 26). It must incorporate the cost for up to 20 copies of all reports and management letters to be submitted. The price sheet must be submitted in the format attached at page F5.

   Price sheets for the preparation of the financial statements for and audit of the Montgomery County Union Employees Deferred Compensation Plan must include:

   - A firm fixed price for the work described in part o) of the Work Statement (see page 26). It must incorporate the cost for up to 20 copies of all reports and management letters to be submitted. The price sheet must be submitted in the format attached at page F6.

Prior to the execution of the contract, the following items must be submitted:

- Minority, Female, Disabled Person Subcontractor Performance Plan (contract value greater than $65,000) – Attachment B,
- Offeror Certification of Cost and Price (contract value greater than $100,000) – Attachment C,
- Certificate of Insurance (see mandatory insurance requirements) - Attachment D. The awardee must provide the applicable insurance coverage and all costs for this coverage must be calculated into the proposal price,
- Photocopies of licenses held by the Offeror (if applicable), and
- An indication of financial responsibility in the form of at least two financial references or credit references.

END SECTION F – PROPOSAL SUBMISSIONS

SECTION G - COMPENSATION

The Contractor will be paid on a monthly basis within 30 days of submission of an acceptable and proper invoice, approved by the County.

SECTION H - CONTRACT ADMINISTRATOR

The Contract Administrator, Office of Legislative Oversight, is the delegated contracting officer. Therefore, the Contract Administrator, Office of Legislative Oversight, must approve in writing: 1) amendments, 2) modifications, 3) changes to the terms or conditions, 4) changes to the minority, female, and disabled subcontractor plans. The contract administrator for any contract(s) resulting from this solicitation will be Leslie Rubin, Office of Legislative Oversight.

The contract administrator's duties include, the following:

1. Serve as liaison between the County Council and Contractor,
2. Give direction to the Contractor to ensure satisfactory and complete performance,
3. Monitor and inspect the Contractor's performance to ensure acceptable timeliness and quality,
4. Serve as Records Custodian for this contract, including documentation of Wage Requirements,
5. Accept or reject the Contractor's performance,
6. Furnish timely written notice of the Contractor's performance failures to the County Council, as appropriate,
7. Prepare required reports,
8. Approve or reject invoices for payment,
9. Recommend contract modifications or terminations to the County Council,
10. Issue notices to proceed, and
11. Monitor and verify compliance with the Minority, Female, Disabled Person Subcontractor Performance Plan.

SECTION I - ETHICS

As a result of being awarded this contract the successful Contractor may be ineligible for the award of related contracts. Montgomery County Code Sections 11B-52 (b) and (c) state:

> A contractor providing an analysis or recommendation to the County concerning a particular matter must not, without first obtaining the written consent of the Chief Administrative Officer:
>
> (1) Assist
>
> (a) another party in the matter; or
> (b) another person if the person has a direct and substantial interest in the matter;
>
> or
>
> (2) Seek or obtain an economic benefit from the matter in addition to payment to the contractor by the County.

SECTION J- COMPUTER RESOURCES SECURITY

The Contractor may be afforded remote access privileges to County Information Resources, or otherwise work on, or interface with, County Information Resources, and must ensure that the County's Information Resources, including electronic data assets, are protected from theft, unauthorized destruction, use, modification, or disclosure as deemed necessary under the County's Information Resources Security Procedure (AP 6-7). The Contractor must adhere to any and all policies and procedures under, or related to, the County's Information Resources Security Procedure (AP 6-7), which is expressly attached to this RFP as Attachment H.

The County's Information Resources Security Procedure (AP 6-7) references the County Computer Security Guideline and the County's Administrative Procedure 6-1. The County Computer Security Guideline (September 2004 version) and Administrative Procedure 6-1 are included in this RFP as Attachment H.

RFP #425820958

ATTACHMENT A

REFERENCES

(must submit at least three)

You are requested to provide references to the County with your proposal. The three (3) references must be from government clients in three (3) different jurisdictions currently being serviced or supplied under similar contracts, or for whom work of a similar scope has been performed within the last year. Names for references shall be of individuals who directly supervised or had direct knowledge of the services or goods provided. Failure of an Offeror to provide the County with references within the time frame as stated herein may result in the Offeror being considered non-responsible.

NAME OF JURISDICTION/OFFICE: _____

ADDRESS: _____

CITY: _____ STATE: _____ ZIP: _____

CONTACT PERSON: _____ TITLE:_____

PHONE: _____

NAME OF JURISDICTION/OFFICE: _____

ADDRESS: _____

CITY: _____ STATE: _____ ZIP: _____

CONTACT PERSON: _____ TITLE:_____

PHONE: _____

NAME OF JURISDICTION/OFFICE: _____

ADDRESS: _____

CITY: _____ STATE: _____ ZIP: _____

CONTACT PERSON: _____ TITLE:_____

PHONE: _____

RFP #425820958

ATTACHMENT B

Minority-Owned Business Addendum to the General Conditions of Contract between County and Contractor, and its companion document "Minority, Female, Disabled Person Subcontractor Performance Plan"

A. While this contract is not subject to the Montgomery County Code and the Montgomery County Procurement Regulations, Offerors for this contract are required to participate in the Minority-Female-Disabled Person (MFD) procurement program.

B. Contractor must subcontract a percentage goals listed below of the total dollar value of the contract, including all modifications and renewals, to certified minority owned businesses. The MFD subcontracting goal may be waived under appropriate circumstances by submission of a letter to the Contract Administrator. The letter must explain why a waiver is appropriate. The Director of the Office of Legislative Oversight or designee may waive, in whole or in part, the MFD subcontracting goal if the Director determines that a waiver is appropriate using guidance from Section 7.3.3.5 of the Montgomery County Procurement Regulations. In determining if a waiver should be granted, the Director may require the Contractor to submit additional information; the Director may require the Contractor to submit some or all of this information on forms approved by the Director.

Below are goals set for each purchasing category for the total value and life of the contract award:

- Construction **27%**
- Professional Services **18%**
- Non-professional Services **25%**
- Goods **14%**

C. The attached MFD Subcontractor Performance Plan, which must be approved by the Contract Administrator, is an integral part of the contract between County and Contractor. In a multi-term contract, Contractor must submit a MFD Subcontract Performance Plan to be in effect for the life of the contract, including any renewal or modification.

D. Contractor must include in each subcontract with a minority owned business a provision that requires the use of binding arbitration with a neutral arbitrator to resolve disputes between the Contractor and the minority owned business subcontractor. This arbitration provision must describe how the cost of dispute resolution will be apportioned; the apportionment must not, in the judgment of the Director, attempt to penalize a minority owned business subcontractor for filing an arbitration claim.

E. County approval of the MFD Subcontractor Performance Plan does not create a contractual relationship between the County and the minority owned business subcontractor.

F. Contractor must notify and obtain prior written approval from the Director regarding any change in the MFD Subcontractor Performance Plan.

G. Before receiving final payment under this contract, Contractor must submit documentation showing compliance with the MFD Subcontracting Performance Plan. Documentation may include, at the direction of the Director, invoices, copies of subcontracts with minority owned businesses, cancelled checks, affidavits executed by minority owned business subcontractors, waivers, and arbitration decisions. The Director may require Contractor to submit periodic reports on a form approved by the Director. The Director may conduct an on-site inspection for the purpose of determining compliance with the MFD Subcontractor Performance Plan. If this is a multi-term contract, final payment means the final payment due for performance rendered for each term of the contract.

If the Contractor fails to submit documentation demonstrating compliance with the MFD Subcontractor Performance Plan, to the satisfaction of the Director, after considering relevant waivers and arbitration decisions, the Contractor is in breach of this contract. In the event of a breach of contract under this addendum, the Contractor must pay to the County liquidated damages equal to the difference between all amounts the Contractor has agreed under its Plan to pay minority owned business subcontractors and all amounts actually paid minority owned business subcontractors with appropriate credit given for any relevant waiver or arbitration decision. Contractor and County acknowledge that damages which would result to the County as a result of a breach under this addendum are difficult to ascertain, and that the liquidated damages provided for in this addendum are fair and reasonable in estimating the damage to the County of a breach of this addendum by Contractor. In addition, the County may terminate the contract. As the result of a breach under this addendum, The Director of the Department of General Services must find the Contractor non-responsible for purposes of future procurement with the County for the ensuing three years.

RFP #425820958

MONTGOMERY COUNTY, MARYLAND

MINORITY, FEMALE, DISABLED PERSON SUBCONTRACTOR PERFORMANCE PLAN

Contractor's Name: _____

Address: _____

City: _____ State: _____ Zip: _____

Phone Number: _____ Fax Number: _____ Email: _____

CONTRACT NUMBER/PROJECT DESCRIPTION: _____

A. Individual assigned by Contractor to ensure Contractor's compliance with MFD Subcontractor Performance Plan:

Name: _____

Title: _____

Address: _____

City: _____ State: _____ Zip: _____

Phone Number: _____ Fax Number: _____ Email: _____

B. This Plan covers the life of the contract from contract execution through the final contract expiration date.

C. The percentage of total contract dollars, including modifications and renewals, to be paid to all certified minority owned business subcontractors, is _____% of the total dollars awarded to Contractor.

D. Each of the following certified minority owned businesses will be paid the percentage of total contract dollars indicated below as a subcontractor under the contract.

I hereby certify that the business(s) listed below are certified by one of the following: Maryland Department of Transportation (MDOT); Virginia Small, Woman and Minority Owned Business (SWAM); Federal SBA (8A); MD/DC Minority Supplier Development Council (MSDC); Women's Business Enterprise National Council (WBENC); or City of Baltimore.
A Certification Letter must be attached. For assistance, call 240-777-9912.

1. Certified by: _____

Subcontractor Name: _____

Title: _____

Address: _____

City: _____ State: _____ Zip: _____

Phone Number: _____ Fax Number: _____ Email: _____

CONTACT PERSON: _____

Circle MFD Type:

AFRICAN AMERICAN	ASIAN AMERICAN	DISABLED PERSON
FEMALE	HISPANIC AMERICAN	NATIVE AMERICAN

The percentage of total contract dollars to be paid to this subcontractor : _____

This subcontractor will provide the following goods and/or services: _____

2. Certified by: _____

Subcontractor Name: _____

Title: _____

Address: _____

City: _____ State: _____ Zip: _____

Phone Number: _____ Fax Number: _____ Email: _____

CONTACT PERSON: _____

Circle MFD Type:

AFRICAN AMERICAN ASIAN AMERICAN DISABLED PERSON
FEMALE HISPANIC AMERICAN NATIVE AMERICAN

The percentage of total contract dollars to be paid to this subcontractor: _____

This subcontractor will provide the following goods and/or services: _____

_____

3. Certified by: _____

Subcontractor Name: _____

Title: _____

Address: _____

City: _____ State: _____ Zip: _____

Phone Number: _____ Fax Number: _____ Email: _____

CONTACT PERSON: _____

Circle MFD Type:

AFRICAN AMERICAN ASIAN AMERICAN DISABLED PERSON
FEMALE HISPANIC AMERICAN NATIVE AMERICAN

The percentage of total contract dollars to be paid to this subcontractor: _____

This subcontractor will provide the following goods and/or services: _____

_____

4. Certified By: _____

Subcontractor Name: _____

Title: _____

Address: _____

City: _____ State: _____ Zip: _____

Phone Number: _____ Fax Number: _____ Email: _____

CONTACT PERSON: _____

Circle MFD Type:

AFRICAN AMERICAN	ASIAN AMERICAN	DISABLED PERSON
FEMALE	HISPANIC AMERICAN	NATIVE AMERICAN

The percentage of total contract dollars to be paid to this subcontractor: _____

This subcontractor will provide the following goods and/or services: _____

_____

E. The following language will be inserted in each subcontract with a certified minority owned business listed in D above, regarding the use of binding arbitration with a neutral arbitrator to resolve disputes with the minority owned business subcontractor; the language must describe how the costs of dispute resolution will be apportioned:

_____

_____

_____

_____

F. Provide a statement below, or on a separate sheet, that summarizes maximum good faith efforts achieved, and/or the intent to increase minority participation throughout the life of the contract or the basis for a full waiver request.

_____

_____

_____

_____

_____

G. A full waiver request must be justified and attached.

Full Waiver Approved:

_____ Date: _____

MFD Program Officer

Partial Waiver Approved:

_____ Date: _____

MFD Program Officer

Full Waiver Approved:

_____ Date: _____

Cherri Branson, Director
Office of Procurement

Partial Waiver Approved:

_____ Date: _____

Cherri Branson, Director
Office of Procurement

The Contractor submits this MFD Subcontractor Performance Plan (Plan Modification No.) in accordance with the Minority Owned Business Addendum to General Conditions of Contract between County and Contractor.

CONTRACTOR SIGNATURE

USE ONE:

1. TYPE CONTRACTOR'S NAME: _____

_____

Signature

_____

Typed Name

_____

Date

2. TYPE CORPORATE CONTRACTOR'S NAME: _____

_____
Signature

_____
Typed Name

_____
Date

I hereby affirm that the above named person is a corporate officer or a designee empowered to sign contractual agreements for the corporation.

_____
Signature

_____
Typed Name

_____
Title

_____
Date

APPROVED:

_____ _____
Cherri Branson, Director, Office of Procurement Date

Section 7.3.3.4(a) of the Procurement Regulations requires:
The Contractor must notify the Contract Administrator of any proposed change to the Subcontractor Performance Plan.

RFP #425820958

ATTACHMENT C

OFFEROR'S CERTIFICATION OF COST AND PRICE

The County Council has the authority to require that contract cost and pricing principles are followed. Cost and Pricing Data must be submitted by Offerors or Contractors in the attached format prior to the execution of any contract or contract amendment based on the following:

1. A competitively negotiated contract valued at more than $100,000.
2. A non-competitive contract valued at more than $50,000.
3. Any contract modification for which the price adjustment is expected to exceed $50,000, except contract modifications that are fully in accordance with the terms and conditions of the contract.
4. Any other contracts or contracts modification, as may be required by the CAO or Director.

OFFEROR'S CERTIFICATION

This cost proposal reflects our best estimates and/or actual costs as of this date and conforms to the cost exhibits and schedules provided by the County Council. By submitting this proposal, the Offeror grants the contracting officer or an authorized representative the right to examine, as the basis for pricing that will permit an adequate evaluation of the proposed price, books, records, documents, and other types of factual information, if specifically referenced or included in the cost proposal.

The Offeror also agrees that the price to the County, including profit or fee, may, at the option of the County Council, be adjusted to reduce the price to the County Council to the extent that the price was based on inaccurate, incomplete, or non-current data supplied by the Offeror.

_____
Name

_____
Title

_____
Name of Firm

_____
Date of Submission

_____
Signature of Authorized Representative

RFP #425820958

COST AND PRICE REQUIREMENTS

By submitting your proposal, you, if selected for negotiation, grant the Contracting Officer or an authorized representative the right to examine those books, records, documents and any other supporting data that will permit adequate evaluation of the proposed price. This right may be exercised at any time prior to award of a contract. The Montgomery County Government may utilize an independent contractor for cost and price analysis or to examine your books and records.

The Cost/price for any resultant contract will be negotiated on the basis of the successful Offeror's normal estimating and/or accounting system or the system set forth in Cost Accounting Standards Board Disclosure Statement as required by Public Law 100-679.

Prior to contract execution, the intended awardee may be required to provide the following information;

A. Latest and previous year's financial statement or profit and loss statement.
B. Burdened rate verification detailing the composition and value of the elements of Fringe Benefits, Overhead, General and Administrative Overhead, Profit or Fee.

RFP #425820958

ATTACHMENT D

MANDATORY INSURANCE REQUIREMENTS

TABLE A. - INSURANCE REQUIREMENTS
(See Provision #21 Under the General Conditions of Contract Between County Council and Contractor)

	CONTRACT DOLLAR VALUES (IN $1,000's)			
	Up to 50	Up to 100	Up to 1,000	Over 1,000
Workers Compensation (for contractors with employees)				
Bodily Injury by:				
Accident (each)	100	100	100	See
Disease (policy limits)	500	500	500	Attachment
Disease (each employee)	100	100	100	
Commercial General Liability minimum combined single limit for bodily injury and property damage per occurrence, including contractual liability, premises and operations, and independent contractors	300	500	1,000	See Attachment
Minimum Automobile Liability (including owned, hired and non-owned automobiles)				
Bodily Injury:				
each person	100	250	500	See
each occurrence	300	500	1,000	Attachment
Property Damage:				
Each occurrence	300	300	300	
Professional Liability* for errors, omissions and negligent acts, per claim and aggregate, with one year discovery period and maximum deductible of $25,000	250	500	1,000	See Attachment

Certificate Holder
Montgomery County Government
ATTN: Leslie Rubin
Contract Administrator
Office of Legislative Oversight
Council Office Building
100 Maryland Avenue, Room 509
Rockville, Maryland 20850-4166
Contract #

*Professional services contracts only

[Remainder of Page Intentionally Left Blank]

RFP #425820958

ATTACHMENT E

Wage Requirements for Services Contract
Addendum to the General Conditions of Contract between County Council and Contractor

A. While this contract is not subject to the Montgomery County Code and the Montgomery County Procurement Regulations, Offerors for this contract are required to certify that they comply with the requirements in Section 11B-33A of the Montgomery County Code.

B. Conflicting requirements (11B-33A (g)): If any federal, state, or County law or regulation requires payment of a higher wage, that law or regulation controls. If any applicable collective bargaining agreement requires payment of a higher wage, that agreement controls.

C. A nonprofit organization that is exempt from the Wage Law under 11B-33A must specify the wage the organization intends to pay to those employees who will perform direct, measurable work under the contract, and any health insurance the organization intends to provide to those employees. Section 11B-33A (b)(3) & (c)(2).

D. A contractor must not split or subdivide a contract, pay an employee through a third party, or treat an employee as a subcontractor or independent contractor, to avoid the imposition of any requirement in 11B-33A.

E. Each contractor and subcontractor must certify that it is aware of and will comply with the applicable wage requirements and keep any verifiable records necessary to show compliance, producible upon request of the Director of the Office of Legislative Oversight.

F. An employer must comply with Section 11B-33A during the initial term of the contract and all subsequent renewal periods, and must pay the adjusted wage rate increase required under 11B-33A (e)(2), if any, which is effective July 1 of each year. The County will adjust the wage rate by the annual average increase in the Consumer Price Index for all urban consumers for the Washington-Baltimore metropolitan area, or successor index, for the previous calendar year and must calculate the adjustment to the nearest multiple of 5 cents.

G. An employer must not discharge or otherwise retaliate against an employee for asserting any right, or filing a complaint of a violation, under the WRL.

H. The sanctions under Section 11B-33 (b), which apply to noncompliance with nondiscrimination requirements, apply with equal force and scope to noncompliance with the wage requirements of 11B-33A.

I. The County may assess liquidated damages for any noncompliance by contractor or its subcontractor with Section 11B-33A based on the rate of 1% per day of the total contract amount, or the estimated annual contract value of a requirements contract, for each day of the violation. This liquidated damages amount includes the amount of any unpaid wages, with interest. In the event of a breach of contract under this paragraph, the Contractor must pay to the County liquidated damages noted above, in addition to any other remedies available to the County. Contractor and County acknowledge that damages that would result to the County as a result of a breach under this paragraph are difficult to ascertain, and that the liquidated damages provided for in this paragraph are fair and reasonable in estimating the damage to the County resulting from a breach of this paragraph by Contractor. If a WRL compliance audit determines that the Contractor has violated requirements of the WRL, including but not limited to the wage requirements, the County may assess the Contractor for the cost incurred by the County in conducting the audit. In addition, the contractor is jointly and severally liable for any noncompliance by a subcontractor. Furthermore, Contractor agrees that an aggrieved employee, as a third-party beneficiary, may by civil action against the violating contractor or subcontractor enforce the payment of wages due under Section 11B-33A and recover from the Contractor or subcontractor any unpaid wages with interest, a reasonable attorney's fee, and damages for any retaliation by the Contractor or subcontractor arising from the employee asserting any right, or filing a complaint of violation, under 11B-33A.

J. The Director may conduct random audits to assure compliance with Section 11B-33A. The Director may conduct an on-site inspection(s) for the purpose of determining compliance. Some of the documents that may be required during an audit are listed on the Living Wage FAQ web page: http://www.montgomerycountymd.gov/PRO/OBRC/LivingWage.html.

K. The Contractor is in breach of this contract if the Contractor fails to submit timely documentation demonstrating compliance with Section 11B-33A to the satisfaction of the Director, including: the Wage Requirements Law Payroll Report Form (PMMD-183), which is required to be submitted by the end of the month (January, April, July, October) following each quarter; documents requested in conjunction with a random or compliance audit being conducted by the County; or documents otherwise requested by the Director. In the event of a breach of contract under this paragraph, or for any other violation of the WRL, the County may assess against, or withhold from payment to, Contractor, the liquidated damages noted in paragraph I. above, in addition to any other remedies available to the County. Contractor and County acknowledge that damages that would result to the County as a result of a breach under this paragraph are difficult to ascertain, and that the liquidated damages provided for in this paragraph are fair and reasonable in estimating the damage to the County resulting from a breach of this paragraph by Contractor.

L. For any questions, please contact the Wage Law Program Manager at 240-777-9918 or WRL@montgomerycountymd.gov .

[Remainder of Page Intentionally Left Blank]

RFP #425820958

Wage Requirements Law Certification

Business Name					
Address					
City		State		Zip Code	
Phone Number		Fax Number			
E-Mail Address					

Provide, in the spaces below, the contact name and information of the individual designated by your firm to monitor your compliance with the County's Wage Requirements Law, unless exempt under Section 11B-33A (b) (see Section B. below):

Contact Name		Title	
Phone Number		Fax Number	
E-mail Address			

In the event that you, the "Offeror," are awarded the contract and become a Contractor, YOU MUST MARK ☑ or ☒ in ALL BOXES BELOW that apply.

☐ A. Wage Requirements Compliance

This Contractor, as a "covered employer", will comply with the requirements under County Code Section 11B-33A, "Wage Requirements" ("Wage Requirements Law" or WRL"). Contractor and its subcontractors will pay all employees not exempt under the WRL, and who perform direct measurable work for the County, the required wage rate effective at the time the work is performed. The offer price(s) submitted under this solicitation include(s) sufficient funds to meet the requirements of the WRL. A "covered employer" must submit (preferably via email) quarterly (by the end of January, April, July, and October for the quarter ending the preceding month) certified payroll records for each payroll period and for all employees of the contractor or a subcontractor performing services under the County contract governed by the Wage Requirements Law, to the Office of Business Relations and Compliance, Attn: Wage Law Program Manager. These payroll records must include the following: name; position/title; gender/race (for contracts awarded after October 1, 2015); daily straight-time hours worked; daily overtime hours worked; straight-time hourly pay rate; overtime hourly pay rate; both employer and employee share of health insurance premium; and total gross wages paid for each period. A sample of the Payroll Report Form can be found at the below link. (http://www.montgomerycountymd.gov/PRO/OBRC/LivingWage.html). In lieu of the Payroll Report Form, payroll registers generally satisfy the requirement. Late submission or non-submission of this information, or any other violation of the WRL, may result in the County withholding contract payments and additional actions by the County, including but not limited to: assessing liquidated damages, terminating the contract, or otherwise taking action to enforce the contract or the Wage Requirements Law. The Contractor must ensure that NO Social Security number of any person, other than the last four digits, is included on the quarterly report.

B. Exemption Status (if applicable)

This Contractor is exempt from Section 11B-33A, "Wage Requirements," because it is:

1. Reserved – [Intentionally left blank].
2. ☐ a contractor who, at the time a contract is signed, has received less than $50,000 from the County in the most recent 12-month period, and will be entitled to receive less than $50,000 from the County under that contract in the next 12-month period. Section 11B-33A (b)(1);
3. ☐ a public entity. Section 11B-33A (b)(2).
4. ☐ a non-profit organization that has qualified for an exemption from federal income taxes under Section 501(c)(3) of the Internal Revenue Code. Section 11B-33A (b)(3) (**must complete item C below**).
5. ☐ an employer expressly precluded from complying with the WRL by the terms of any federal or state law, contract, or grant. Section 11B-33A (b)(7) (**must specify the law, or furnish a copy of the contract or grant**).

☐ C. Nonprofit Wage & Health Information

This Contractor is a non-profit organization that is exempt from coverage under Section 11B-33A (b)(3). Accordingly, the contractor has completed the 501 (c)(3) Nonprofit Organization's Employee's Wage and Health Insurance Form, which is attached. See Section11B-33A (c)(2).

☐ D. Nonprofit's Comparison Price(s) (if desired)

This Contractor is a non-profit organization that is opting to pay its covered employees the hourly rate specified in the wage requirements. Accordingly, Contractor is duplicating the blanket-cost quotation sheet on which it is submitting its price(s) in the RFP, and is submitting on this duplicate form its price(s) to the County had it not opted to pay its employees the hourly rate specified in the WRL. For proposal evaluation purposes, this price(s) will be compared to price(s) of another nonprofit organization(s) that is paying its employees an amount consistent with its exemption from paying the hourly rate under the WRL. This revised information on the duplicate cost sheet must be clearly marked as your nonprofit organization comparison price(s). In order for the County to compare your price(s), the revised information on the duplicate cost sheet must be submitted with your offer on or before the offer opening date, must show how the difference between your nonprofit organization price(s) and other organization comparison price(s) was calculated. Section 11B-33A (c)(2).

☐ E. Wage Requirements Law Reduction (not applicable after July 22, 2015)

This Contractor is a "covered employer", and it desires to reduce its hourly rate paid under the WRL by an amount equal to, or less than, the per employee hourly cost of the employer's share of the health insurance premium. Contractor certifies that the per employee hourly cost of the employer's share of the premium for that insurance is: **$** . Section 11B-33A (d) & (e).

☐ F. Sole Proprietorship

Sole Proprietorships are subject to the Wage Requirements Law. In order to be excused from the posting and reporting requirements of the WRL, the individual who is the sole proprietor must sign the certifications below in order to attest to the fact that the Sole Proprietorship:

(1) is aware of, and will comply with, the Wage Requirements Law;
(2) has no employees other than the sole proprietor; and
(3) will inform the Montgomery County Office of Business Relations and Compliance if the sole proprietor employs any workers other than the sole proprietor.

Contractor Certification

CONTRACTOR SIGNATURE: Contractor submits this certification form in accordance with Section 11B-33A of the Montgomery County Code. Contractor certifies that it, and any and all of its subcontractors that perform services under the resultant contract with the County, adheres to Section 11B-33A of the Montgomery County Code.

Authorized Signature		Title of Authorized Person	
Typed or printed name		Date	

RFP #425820958

501(c)(3) Nonprofit Organization's Employee's Wage and Health Insurance Form

Business Name					
Address					
City		State		Zip Code	
Phone Number		Fax Number		E-Mail	

Please provide below the employee labor category of all employee(s) who will perform direct measurable work under this contract, the hourly wage the organization pays for that employee labor category, and any health insurance the organization intends to provide for that employee labor category:

Employee Labor Category	Wage per Hour	Name of Health Insurance Provider(s) and Plan Name* (e.g. ABC Insurer, Inc. , HMO Medical and Dental)

* IF NO HEALTH INSURANCE PLAN IS PROVIDED PLEASE STATE "NONE".

RFP #425820958

Attachment F
Price Sheets

Audit of the County's Financial Statements **Section C – Scope of Services, Work Statement Parts a) through g)**				
Name and Address of Offeror/Subcontractor		**Proposal Date:** **Service Being Furnished:**		
Direct Labor	**Hours**	**Hourly Rate**	**Cost**	**Totals**
Partner				
Manager				
Senior				
Staff Auditor				
Other (specify)				
Direct Labor Cost Total				**$**
Indirect Costs (specify indirect cost pools)	**Rate**	**Base**	**Cost**	
Indirect Costs Total				**$**
Subcontracts (company name – services)			**Cost**	
Subcontracts Cost Total				$
Other Costs (specify categories)			**Cost**	
Other Costs Total				**$**
Total Cost				**$**
Profit				**$**
Total Price Proposed				**$**

Attachment F (continued)
Price Sheets

Audit of the County's Financial Statements **Section C – Scope of Services, Work Statement Part h)**	
Name and Address of Offeror/Subcontractor	**Proposal Date:** **Service Being Furnished:**

Direct Labor	**Hours**	**Hourly Rate**	**Cost**	**Totals**
Partner				
Manager				
Senior				
Staff Auditor				
Other (specify)				
Direct Labor Cost Total				**$**
Indirect Costs (specify indirect cost pools)	**Rate**	**Base**	**Cost**	
Indirect Costs Total				**$**
Subcontracts (company name – services)			**Cost**	
Subcontracts Cost Total				$
Other Costs (specify categories)			**Cost**	
Other Costs Total				**$**
Total Cost				**$**
Profit				**$**
Total Price Proposed				**$**

RFP #425820958

Attachment F (continued)
Price Sheets

Audit of the County's Financial Statements **Section C – Scope of Services, Work Statement Part i)**				
Name and Address of Offeror/Subcontractor		**Proposal Date:** **Service Being Furnished:**		
Direct Labor	**Hours**	**Hourly Rate**	**Cost**	**Totals**
Partner				
Manager				
Senior				
Staff Auditor				
Other (specify)				
Direct Labor Cost Total				**$**
Indirect Costs (specify indirect cost pools)	**Rate**	**Base**	**Cost**	
Indirect Costs Total				**$**
Subcontracts (company name – services)			**Cost**	
Subcontracts Cost Total				$
Other Costs (specify categories)			**Cost**	
Other Costs Total				**$**
Total Cost				**$**
Profit				**$**
Total Price Proposed				**$**

Audit of the County's Financial Statements **Section C – Scope of Services, Work Statement Part j)**	
Name and Address of Offeror/Subcontractor	**Proposal Date:** **Services Being Furnished:**
Auditing Services	
Staff Level	**Fixed Hourly Rate**
Partner	
Manager	
Senior	
Staff Auditor	
Specialist/Other (specify)	
Alternate Composite Rate (when already on site)	
Accounting Services	
Staff Level	**Fixed Hourly Rate**
Partner	
Manager	
Senior	
Staff Auditor	
Specialist/Other (specify)	
Alternate Composite Rate (when already on site)	
Comfort or Consent Letters	
	Fixed Fee Per Letter
Comfort Letter	
Consent Letter	

Attachment F (continued)
Price Sheets

Audit of the Employee Retirement Plans Financial Statements **Section C – Scope of Services, Work Statement Parts k) through n)**				
Name and Address of Offeror/Subcontractor		**Proposal Date:** **Service Being Furnished:**		
Direct Labor	**Hours**	**Hourly Rate**	**Cost**	**Totals**
Partner				
Manager				
Senior				
Staff Auditor				
Other (specify)				
Direct Labor Cost Total				**$**
Indirect Costs (specify indirect cost pools)	**Rate**	**Base**	**Cost**	
Indirect Costs Total				**$**
Subcontracts (company name – services)			**Cost**	
Subcontracts Cost Total				$
Other Costs (specify categories)			**Cost**	
Other Costs Total				**$**
Total Cost				**$**
Profit				**$**
Total Price Proposed				**$**

RFP #425820958

Attachment F (continued)
Price Sheets

Preparation and Audit of the Montgomery County Union Employees Deferred Compensation Plan Financial Statements **Section C – Scope of Services, Work Statement Part o)**				
Name and Address of Offeror/Subcontractor		**Proposal Date:** **Service Being Furnished:**		
Direct Labor	**Hours**	**Hourly Rate**	**Cost**	**Totals**
Partner				
Manager				
Senior				
Staff Auditor				
Other (specify)				
Direct Labor Cost Total				**$**
Indirect Costs (specify indirect cost pools)	**Rate**	**Base**	**Cost**	
Indirect Costs Total				**$**
Subcontracts (company name – services)			**Cost**	
Subcontracts Cost Total				$
Other Costs (specify categories)			**Cost**	
Other Costs Total				**$**
Total Cost				**$**
Profit				**$**
Total Price Proposed				**$**

RFP #425820958

Attachment G
Business Associate Agreement

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (the "Agreement") is made by and between Montgomery County, Maryland (hereinafter referred to as "Covered Entity"), and _____ (hereinafter referred to as "Business Associate"). Covered Entity and Business Associate shall collectively be known herein as the "Parties."

I. GENERAL

A. Covered Entity has a business relationship with Business Associate that is memorialized in Montgomery County Contract # _____ (the "Underlying Agreement"), pursuant to which Business Associate may be considered a "business associate" of Covered Entity as defined in the Health Insurance Portability and Accountability Act of 1996, including all pertinent regulations (45 CFR Parts 160 and 164), issued by the U.S. Department of Health and Human Services, including Subtitle D of the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), as codified in Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111–5), and including any and all applicable Privacy, Security, Enforcement, or Notice (Breach Notification) Rules or requirements (collectively, "HIPAA"), as all are amended from time to time; and

B. The performance of the Underlying Agreement may involve the creation, exchange, or maintenance of Protected Health Information ("PHI") as that term is defined under HIPAA; and

C. For good and lawful consideration as set forth in the Underlying Agreement, Covered Entity and Business Associate enter into this Agreement for the purpose of ensuring compliance with the requirements of HIPAA; and

D. This Agreement articulates the obligations of the Parties as to use and disclosure of PHI. It does not affect Business Associate's obligations to comply with the the Maryland Confidentiality of Medical Records Act (Md. Code Ann., Health-General I §§4-301 *et seq*.) ("MCMRA") or other applicable law with respect to any information the County may disclose to Business Associate as part of Business Associate's performance of the Underlying Agreement; and

E. This Agreement supersedes and replaces any and all Business Associate Agreements the Covered Entity and Business Associate may have entered into prior to the date hereof; and

F. The above premises having been considered and incorporated by reference into the sections below, the Parties, intending to be legally bound, agree as follows:

II. DEFINITIONS.

A. The terms used in this Agreement have the same meaning as the definitions of those terms in HIPAA. In the absence of a definition in HIPAA, the terms have their commonly understood meaning.

B. Consistent with HIPAA, and for ease of reference, the Parties expressly note the definitions of the following terms:

1. "Breach" is defined at 45 CFR § 164.402.

2. **"**Business Associate" is defined at 45 CFR § 160.103, and in reference to the party to this Agreement, shall mean [Insert Name of Business Associate].

3. "Covered Entity" is defined at 45 CFR § 160.103, and in reference to the party to this Agreement, shall mean the County.

4. "Designated Record Set" is defined at 45 CFR §164.501.

5. "Individual" is defined at 45 CFR §§ 160.103, 164.501 and 164.502(g), and includes a person who qualifies as a personal representative.

6. "Protected Health Information" or "PHI" is defined at 45 CFR § 160.103.

7. "Required By Law" is defined at 45 CFR § 164.103.

8. "Secretary" means the Secretary of the U.S. Department of Health and Human Services or designee.

9. "Security Incident" is defined at 45 CFR § 164.304.

10. "Unsecured Protected Health Information" or "Unsecured PHI" means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology, as specified by the Secretary in the guidance as noted under the HITECH Act, section 13402(h)(1) and (2) of Public Law 111-5, codified at 42 U.S.C. § 17932(h)(1) and (2), and as specified by the Secretary in 45 CFR 164.402.

III. PERMISSIBLE USE AND DISCLOSURE OF PHI

A. Except as otherwise limited in this Agreement, or by privilege, protection, or confidentiality under HIPAA, MCMRA, or other applicable law, Business Associate may use or disclose (including permitting acquisition or access to) PHI to perform applicable functions, activities, or services for, or on behalf of, Covered Entity as specified in the Underlying Agreement. Moreover, the provisions of HIPAA are expressly incorporated by reference into, and made a part of, this Agreement.

B. Business Associate may use or disclose (including permitting acquisition or access to) PHI only as permitted or required by this Agreement or as Required By Law.

C. Business Associate is directly responsible for full compliance with the relevant requirements of HIPAA.

D. Business Associate must not use or disclose (including permitting acquisition or access to) PHI other than as permitted or required by this Agreement or HIPAA, and must use or disclose PHI only in a manner consistent with HIPAA. As part of this, Business Associate must use appropriate safeguards to prevent use or disclosure of PHI that is not permitted by this Agreement or HIPAA. Furthermore, Business Associate must take reasonable precautions to protect PHI from loss, misuse, and unauthorized access, disclosure, alteration, and destruction.

E. Business Associate must implement and comply with administrative, physical, and technical safeguards governing the PHI, in a manner consistent with HIPAA, that reasonably and appropriately protect the confidentiality, integrity, and availability of the PHI that it creates, receives, maintains, or transmits on behalf of Covered Entity.

F. Business Associate must immediately notify Covered Entity, in a manner consistent with HIPAA, of: (i) any use or disclosure of PHI not provided for by this Agreement, including a Breach of PHI of which it knows or by exercise of reasonable diligence would have known, as required at 45 CFR §164.410; and, (ii) any Security Incident of which it becomes aware as required at 45 CFR §164.314(a)(2)(i)(C). Business Associate's notification to Covered Entity required by HIPAA and this Section III.F must:

1. Be made to Covered Entity without unreasonable delay and in no case later than 14 calendar days after Business Associate: a) knows, or by exercising reasonable diligence would have known, of a Breach, b) becomes aware of a Security Incident, or c) becomes aware of any use or disclosure of PHI not provided for by this Agreement;

2. Include the names and addresses of the Individual(s) whose PHI is the subject of a Breach, Security Incident, or use or disclosure of PHI not provided for by this Agreement. In addition, Business Associate must provide any additional information reasonably requested by Covered Entity for purposes of investigating the Breach, Security Incident, or use or disclosure of PHI not provided for by this Agreement;

3. Be in substantially the same form as Exhibit A hereto;

4. Include a brief description of what happened, including the date of the Breach, Security Incident, or use or disclosure of PHI not provided for by this Agreement, if known, and the date of the discovery of the Breach, Security Incident, or use or disclosure of PHI not provided for by this Agreement;

5. Include a description of the type(s) of Unsecured PHI that was involved in the Breach, Security Incident, or use or disclosure of PHI not provided for by this Agreement (such as full name, Social Security number, date of birth, home address, account number, disability code, or other types of information that were involved);

6. Identify the nature and extent of the PHI involved, including the type(s) of identifiers and the likelihood of re identification;

7. If known, identify the unauthorized person who used or accessed the PHI or to whom the disclosure was made;

8. Articulate any steps the affected Individual(s) should take to protect him or herself from potential harm resulting from the Breach, Security Incident, or use or disclosure of PHI not permitted by this Agreement;

9. State whether the PHI was actually acquired or viewed;

10. Provide a brief description of what the Covered Entity and the Business Associate are doing to investigate the Breach, Security Incident, or use or disclosure of PHI not provided for by this Agreement, to mitigate losses, and to protect against any further Breach, Security Incident, or use or disclosure of PHI not provided for by this Agreement;

11. Note contact information and procedures for an Individual(s) to ask questions or learn additional information, which must include a toll-free telephone number of Business Associate, along with an e-mail address, Web site, or postal address;

and

12. Include a draft letter for the Covered Entity to utilize, in the event Covered Entity elects, in its sole discretion, to notify the Individual(s) that his or her PHI is the subject of a Breach, Security Incident, or use or disclosure of PHI not provided for by this Agreement that includes the information noted in Section III.F.4 – III.F.11 above.

G. Business Associate must, and is expected to, directly and independently fulfill all notification requirements under HIPAA.

H. In the event of a Breach, Security Incident, or use or disclosure of PHI not provided for by this Agreement, Business Associate must mitigate, to the extent practicable, any harmful effects of said disclosure that are known to it.

I. In accordance with 45 CFR §§ 164.502(e)(1)(ii) and 164.308(b)(2), Business Associate agrees to ensure that any agent, subcontractor, or employee to whom it provides PHI (received from, or created or received by, Business Associate on behalf of Covered Entity) agrees to the same restrictions, conditions, and requirements that apply through this Agreement to Business Associate with respect to such information.

J. Business Associate must ensure that any contract or other arrangement with a subcontractor meets the requirements of paragraphs 45 CFR §164.314(a)(2)(i) and (a)(2)(ii) required by 45 CFR § 164.308(b)(3) between a Business Associate and a subcontractor, in the same manner as such requirements apply to contracts or other arrangements between a Covered Entity and Business Associate.

K. Pursuant to 45 CFR § 164.502(a)(4)(ii), Business Associate must disclose PHI to the Covered Entity, Individual, or Individual's designee, as necessary to satisfy a Covered Entity's obligations under § 164.524(c)(2)(ii) and (3)(ii) with respect to an individual's request for an electronic copy of PHI.

L. To the extent applicable, Business Associate must provide access to PHI in a Designated Record Set at reasonable times, at the request of Covered Entity or as directed by Covered Entity, to an Individual specified by Covered Entity in order to meet the requirements under 45 CFR § 164.524.

M. A Business Associate that is a health plan, excluding an issuer of a long-term care policy falling within paragraph (1)(viii) of the definition of health plan, must not use or disclose PHI that is genetic information for underwriting purposes, in accordance with the provisions of 45 CFR 164.502.

N. To the extent applicable, Business Associate must make any amendment(s) to PHI in a Designated Record Set that Covered Entity directs or agrees to, pursuant to 45 CFR § 164.526, at the request of Covered Entity or an Individual.

O. Business Associate must, upon request with reasonable notice, provide Covered Entity access to its premises for a review and demonstration of its internal practices and procedures for safeguarding PHI.

P. Business Associate must, upon request and with reasonable notice, furnish to Covered Entity security and privacy audit results, risk analyses, security and privacy policies and procedures, details of previous Breaches and Security Incidents, and documentation of controls.

Q. Business Associate must also maintain records indicating who has accessed PHI about an Individual in an electronic designated record set and information related to such access, in accordance with 45 C.F.R. § 164.528. Business Associate must document such disclosures of PHI and information related to such disclosures as would be required for a Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528. Should an Individual make a request to Covered Entity for an accounting of disclosures of his or her PHI pursuant to 45 C.F.R. § 164.528, Business Associate must promptly provide Covered Entity with information in a format and manner sufficient to respond to the Individual's request.

R. Business Associate must, upon request and with reasonable notice, provide Covered Entity with an accounting of uses and disclosures of PHI that was provided to it by Covered Entity.

S. Business Associate must make its internal practices, books, records, and any other material requested by the Secretary relating to the use, disclosure, and safeguarding of PHI received from Covered Entity available to the Secretary for the purpose of determining compliance with HIPAA. Business Associate must make the aforementioned information available to the Secretary in the manner and place as designated by the Secretary or the Secretary's duly appointed delegate. Under this Agreement, Business Associate must comply and cooperate with any request for documents or other information from the Secretary directed to Covered Entity that seeks documents or other information held or controlled by Business Associate.

T. Business Associate may use PHI to report violations of law to appropriate Federal and State authorities, consistent with 42 C.F.R. § 164.502(j)(1).

U. Except as otherwise limited in this Agreement, Business Associate may disclose PHI for the proper management and administration of Business Associate or the Underlying Agreement, provided that disclosures are Required By Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and be used or further disclosed only as Required By Law or for the limited purpose for which it was disclosed to the person, and the person must agree to notify Business Associate of any instance of any Breach, Security Incident, or use or disclosure of PHI not provided for by this Agreement of which it is aware in which the confidentiality of the information has been breached.

V. Business Associate understands that, pursuant to 45 CFR § 160.402, the Business Associate is liable, in accordance with the Federal common law of agency, for a civil money penalty for a violation of the HIPAA rules based on the act or omission of any agent of the Business Associate, including a workforce member or subcontractor, acting within the scope of the agency.

IV. TERM AND TERMINATION.

A. Term. The Term of this Agreement shall be effective as of the effective date of the Underlying Agreement, and shall terminate: (1) when all of the PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity; or, (2) if it is infeasible to return or destroy PHI, in accordance with the termination provisions in this Article IV.

B. Termination for Cause. Upon Covered Entity's knowledge of a material breach of this Agreement by Business Associate, Covered Entity shall:

1. Provide an opportunity for Business Associate to cure the breach or end the violation and, if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity, have the right to terminate this Agreement and to terminate the Underlying Agreement, and shall report the violation to the Secretary;

2. Have the right to immediately terminate this Agreement and the Underlying Agreement if Business Associate has breached a material term of this Agreement and cure is not possible, and shall report the violation to the Secretary; or

3. If neither termination nor cure is feasible, report the violation to the Secretary.

4. This Article IV, Term and Termination, Paragraph B, is in addition to the provisions set forth in Paragraph 27, Termination for Default of the General Conditions of Contract Between County and Contractor, attached to the Underlying Agreement, in which "Business Associate" is "Contractor" and "Covered Entity" is "County" for purposes of this Agreement.

C. Effect of Termination.

1. Except as provided in Section IV.C.2, upon termination or cancellation of this Agreement, for any reason, Business Associate must return or destroy all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision applies to PHI that is in the possession of a subcontractor(s), employee(s), or agent(s) of Business Associate. Business Associate must not retain any copies of the PHI.

2. In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate must provide to Covered Entity written notification of the nature of the PHI and the conditions that make return or destruction infeasible. After written notification that return or destruction of PHI is infeasible, Business Associate must extend the protections of this Agreement to such PHI and limit further use(s) and disclosure(s) of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI. Notwithstanding the foregoing, to the extent that it is not feasible to return or destroy such PHI, the terms and provisions of this Agreement survive termination of this Agreement with regard to such PHI.

3. Should Business Associate violate this Agreement, HIPAA, the Underlying Agreement, the MCMRA, or other applicable law, Covered Entity has the right to immediately terminate any contract then in force between the Parties, including the Underlying Agreement.

V. CONSIDERATION. Business Associate recognizes that the promises it has made in this Agreement shall, henceforth, be reasonably, justifiably, and detrimentally relied upon by Covered Entity in choosing to continue or commence a business relationship with Business Associate.

VI. CAUSES OF ACTION IN THE EVENT OF BREACH. As used in this paragraph, the term "breach" has the meaning normally ascribed to that term under the Maryland law related to contracts, as opposed to the specific definition under HIPAA related to PHI. Business Associate hereby recognizes that irreparable harm will result to Covered Entity in the event of breach by Business Associate of any of the covenants and assurances contained in this Agreement. As such, in the event of breach of any of the covenants and assurances contained in this Agreement, Covered Entity shall be entitled to enjoin and restrain Business Associate from any continued violation of this Agreement. Furthermore, in the event of breach of this Agreement by Business Associate, Covered Entity is entitled to reimbursement and indemnification from Business Associate for Covered Entity's reasonable attorneys' fees and expenses and costs that were reasonably incurred as a proximate result of Business Associate's breach. The causes of action contained in this Article VI are in addition to (and do not supersede) any action for damages and/or any other cause of action Covered Entity may have for breach of any part of this Agreement. Furthermore, these provisions are in addition to the provisions set forth in Paragraph 18, "Indemnification", of the General Conditions of Contract Between County and Contractor, attached to the Underlying Agreement in which "Business Associate" is "Contractor" and "Covered Entity" is "County", for purposes of this Agreement.

VII. MODIFICATION; AMENDMENT. This Agreement may be modified or amended only through a writing signed by the Parties and, thus, no oral modification or amendment hereof shall be permitted. The Parties agree to take such action as is necessary to amend this Agreement, from time to time, as is necessary for Covered Entity to comply with the requirements of HIPAA, including its Privacy, Security, and Notice Rules.

VIII. INTERPRETATION OF THIS AGREEMENT IN RELATION TO OTHER AGREEMENTS BETWEEN THE PARTIES. Should there be any conflict between the language of this Agreement and any other contract entered into between the Parties (either previous or subsequent to the date of this Agreement), the language and provisions of this Agreement, along with the Underlying Agreement, shall control and prevail unless the Parties specifically refer in a subsequent written agreement to this Agreement, by its title, date, and substance and specifically state that the provisions of the later written agreement shall control over this Agreement and Underlying Agreement. In any event, any agreement between the Parties, including this Agreement and Underlying Agreement, must be in full compliance with HIPAA, and any provision in an agreement that fails to comply with HIPAA will be deemed separable from the document, unenforceable, and of no effect.

IX. COMPLIANCE WITH STATE LAW. The Business Associate acknowledges that by accepting the PHI from Covered Entity, it becomes a holder of medical records information under the MCMRA and is subject to the provisions of that law. If HIPAA conflicts with another applicable law regarding the degree of protection provided for Protected Health Information, Business Associate must comply with the more restrictive protection requirement.

X. MISCELLANEOUS.

A. Ambiguity. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with HIPAA.

B. Regulatory References. A reference in this Agreement to a section in HIPAA means the section in effect, or as amended.

C. Notice to Covered Entity. Any notice required under this Agreement to be given Covered Entity shall be made in writing to:

Joy Page, Esq.
Deputy Privacy Official
Montgomery County, Maryland
401 Hungerford Drive, 7th Floor
Rockville, Maryland 20850
(240) 777-3247 (Voice)
(240) 777- 3099 (Fax)

Notice to Business Associate. Any notice required under this Agreement to be given Business Associate shall be made in writing to:

Address: _____

_____

Attention: _____

Phone: _____

D. Maryland Law. This Agreement is governed by, and shall be construed in accordance with, applicable federal law and the laws of the State of Maryland, without regard to choice of law principles.

E. Incorporation of Future Amendments. Other requirements applicable to Business Associates under HIPAA are incorporated by reference into this Agreement.

F. Penalties for HIPAA Violation. In addition to that stated in this Agreement, Business Associate may be subject to civil and criminal penalties noted under HIPAA, including the same HIPAA civil and criminal penalties applicable to a Covered Entity.

IN WITNESS WHEREOF and acknowledging acceptance and agreement of the foregoing, the Parties affix their signatures hereto.

(INSERT NAME OF BUSINESS ASSOCIATE)	MONTGOMERY COUNTY, MARYLAND
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

RFP #425820958

EXHIBIT A

FORM OF NOTIFICATION

This notification is made pursuant to Section III.F of the Business Associate Agreement between:

- Montgomery County, Maryland, (the "County") and
- _____(Business Associate).

Business Associate hereby notifies the County that there has been a Breach, Security Incident, or use or disclosure of PHI not provided for by the Business Associate Agreement (an "Incident") that Business Associate has used or has had access to under the terms of the Business Associate Agreement.

Description of the Incident:

_____

_____

Date of the Incident: _____

Date of discovery of the Incident: _____

Does the Incident involve 500 or more individuals? Yes/No

If yes, do the people live in multiple states? Yes/No

Number of individuals affected by the Incident:

_____

Names and addresses of individuals affected by the Incident:

(Attach additional pages as necessary)_____

The types of unsecured PHI that were involved in the Incident (such as full name, Social Security number, date of birth, home address, account number, or disability code):

_____
_____

Description of what Business Associate is doing to investigate the Incident, to mitigate losses, and to protect against any further Incidents:

_____

_____

_____

Contact information to ask questions or learn additional information:

Name: _____

Title: _____

Address: _____

_____

Email Address: _____

Phone Number: _____

Attachment H

MONTGOMERY COUNTY ADMINISTRATIVE PROCEDURE

Offices of the County Executive • 101 Monroe Street • Rockville, Maryland 20850

NO. 6-1

PAGE 1 OF 8

DATE 9/2/10

CAO APPROVAL

TITLE

Use of County-Provided Internet, Intranet, and E-mail Services

PURPOSE

1.0 To establish an administrative procedure governing the use of County-provided Internet, intranet, and electronic mail services by County employees. The County maintains intranet and Internet access for its employees for the purpose of improving productivity, professional development, and the level of service to the people of our community.

DEFINITIONS

2.0 Department of Technology Services (DTS) - A department in the executive branch that is responsible for automated information systems and telecommunications technology.

2.1 CIO - Chief Information Officer and DTS Department Head

2.2 Personal Use – Activity that is conducted for purposes other than accomplishing official or otherwise authorized activity.

POLICY

3.0 Internet, intranet, and electronic mail (email) services are provided to County employees and persons legitimately affiliated with the business of the County government for the efficient exchange of information and the completion of assigned responsibilities that are consistent with the County's purposes.

3.1 Employees must use County-provided Internet, intranet, and email services responsibly and professionally, and must not use Internet, intranet, or email services in a manner that violates any applicable federal, State, or Montgomery County law, regulation, or policy, including those contained in the County's Administrative Procedures.

3.2 A County employee may use County-provided Internet, intranet, or email services for personal purposes on only a limited, reasonable basis, and in accordance with this administrative procedure. However, employees must act reasonably to minimize personal use of County-provided Internet, intranet, and email services. Personal use of County Internet, intranet or email services by employees should mainly be during personal time (before and after work or during lunch time). Such use must be kept to a minimum, must not increase or create additional expense to the County and must not disrupt the conduct of service or performance of official duties.

3.3 An employee's use of County-provided Internet, intranet, or email services indicates consent to this administrative procedure, and to the County's access and monitoring, for legitimate business purposes (including a non-investigatory work-related search or investigatory search of suspected work-related misfeasance), of his/her electronically stored email messages and computer files, and any other data related to the employee's use of the County's Internet, intranet, and email services.

3.4 Any employee who is in violation of this administrative procedure may be subject to disciplinary action, including dismissal, and other legal remedies available to the County, in accordance with applicable federal, State, or Montgomery County laws and regulations, including Personnel laws and Regulations, and Ethics Laws, currently codified at Chapter 33, Appendix F, and Chapter 19A of the County Code, respectively, and applicable collective bargaining agreements, as amended.

GENERAL

CONNECTING TO INTERNET, INTRANET, AND EMAIL SERVICES

4.0 County employees may connect to County-provided Internet, intranet, or email services only through:

A. Personal Computers (PCs) such as desktops and laptops connected to the County's computer network via the County's secure enterprise Internet service connection; or

B. Stand-alone (non network-connected or temporarily disconnected) PCs via a private Internet Service Provider (ISP), such as America On-Line (AOL), or via a DTS-sanctioned remote access method.

4.1 Any PC that connects to County-provided Internet, intranet, or email services must have up-to-date antivirus software and current updates for Windows operating system software installed on it and must be configured to actively protect against virus infections and periodically scan the PC to check for viruses.

4.2 Costs incurred by the County for ISP connections to stand-alone PCs are the responsibility of the using department. Employees must obtain department approval prior to obtaining a County-provided ISP connection.

PROHIBITED USER CONDUCT

4.3 Employees must use County-provided Internet, intranet, and email services in accordance with this administrative procedure and all applicable laws, regulations, and policies. Prohibited conduct, including personal use, includes:

A. Accessing, sending, forwarding, storing, or saving on County PCs or servers any material that is offensive, demeaning or disruptive, including messages that are inconsistent with the County's policies concerning "Equal Employment Opportunity" and "Sexual Harassment and Other Unlawful Harassment," for any reason other than for purposes of eliminating this type of material from County systems. The act of inadvertently opening an email that contains this type of material does not, itself, constitute a violation of this policy.

B. Personal use beyond that permitted by this policy.

C. Any use prohibited by federal, State, or County law.

D. Employees may not modify computer equipment for personal purposes. This would include loading of personal software, non-County supplied software; "shareware" and/or "freeware"; animated (executable) screen savers or peer-to-peer software packages. Examples of inappropriate personal configuration include adding unauthorized wireless network cards, use of external storage devices that contain applications, and communications or video components not supplied or tested by the County.

E. Using the County's Internet, intranet, or email services to gain unauthorized access to County or other system resources.

F. Using the County's Internet, intranet, or email services for gambling or other illegal or County-prohibited activities.

G. Using the County's Internet, intranet, or email services for private gain or profit.

H. Infringing upon computer software and data protected by copyright intellectual property rights and/or license laws.

I. Using the County Internet, intranet, or email services or applications to publish and/or represent (expressly or implicitly) personal or unofficial opinions as those of the County.

J. Any personal use that could cause congestion, delay or disruption of service to any County system or equipment. This may include, but not limited to:

1. "Chain" or unnecessary "Reply All" emails; and
2. Downloads of video, sound or other large, non-work related files.

K. Sending broadcast messages to all, or the majority of, County e-mail users without obtaining prior approval from the Chief Administrative Officer (CAO), in accordance with County information technology policies and procedures.

COUNTY OWNERSHIP, MONITORING, CONTROL, AND DISCLOSURE

4.4 All County-provided electronic systems, hardware, software, temporary or permanent files and any related systems or devices used in the transmission, receipt or storage of Internet, intranet, or email communications are the property of, or licensed to, the County.

4.5 Any information transmitted or received by employees using the County's Internet, intranet, and email services, or stored on the County's computer resources, is the property of the County and, therefore, is not considered private. This includes email from an employee's personal account, such as Hotmail or AOL, if that email is stored on the County's computer resources.

4.6 Internet, intranet, and email electronic files and messages may be retrieved from storage by the County and its agents without prior notice to an employee, even if the electronic files and messages have been deleted by the sender or receiver. These messages and files may also be used by the County in disciplinary or other proceedings.

4.7 Employees must take appropriate measures to prevent unauthorized access to confidential information when using the County's Internet, intranet, and email services, in accordance with applicable federal, State, or Montgomery County laws, regulations, or policies regarding confidential information.

4.8 The County may monitor an employee's use of County-provided Internet, intranet, and email services, and may access an employee's email messages and computer files in its sole discretion, when there is a legitimate business purpose (including a non-investigatory work-related search or investigatory search of suspected work-related misfeasance). This includes access to email messages from an employee's personal email account, such as Hotmail or AOL, if the personal email is stored on the County's computer resources.

4.9 Upon the approval of the email user's department head and the CIO, system administrators in DTS or the email user's department may access an employee's email messages and computer files related to the employee's use of the County's Internet, intranet, and email services. The existence of privately held passwords and "message delete" functions do not restrict or eliminate the County's ability or right to access this information.

4.10 The County may monitor or control the flow of Internet/intranet and email traffic over the County's network for security or network management reasons, or for other legitimate business purposes.

4.11 The County may be compelled to access and disclose to third parties messages sent over its Internet, intranet, or email systems, in accordance with the Maryland Public Information Act (MPIA), Maryland Code Ann., State Gov't §§ 10-611 to 10-628 (1998 Repl. Vol.). The MPIA applies to an electronically stored email message or a hard copy of the message in the custody and control of a public officer or employee, if the message is related to the conduct of public business. 81 Op. Att'y Gen, Op No. 96-016, 1996 WL 305985 (1996).

RESPONSIBILITIES

5.0 Department of Technology Services

A. Provide a 24-hour, 7 day-a-week secure, high-speed enterprise connection to Internet, intranet, and email services.

B. Notify users of County-provided Internet, intranet, and email services when those services will be unavailable for system or network maintenance.

C. Provide operating system and anti-virus software for all County-owned PCs, and manage software configurations, including operating system and anti-virus, for all County-owned PCs connected to the County's network.

D. Accept help desk calls when a County employee or department notes a problem with County-provided Internet, intranet, or email services, and distribute information, updates, and/or resolutions, as appropriate.

E. Maintain the current version of this administrative procedure, in accordance with Administrative Procedure 6-6, Information Technology Policies and Procedures Manual.

F. Provide CIO approval or denial of a department head's request to monitor an employee's use of County-provided Internet, intranet, and email services, or to access an employee's email messages and computer files.

G. Provide information to a department head regarding an employee's use of County-provided Internet, intranet, and email services, when directed by the CIO to do so.

5.1 Department

A. Ensure that employees are informed of, and comply with, this administrative procedure.

B. Responsible to ensure the appropriate use of department resources, including IT and official employee time.

C. Ensure that this administrative procedure is incorporated by reference into all contracts in which the County is to provide contactors or volunteers with the use of its Internet, intranet, or email services to conduct the County's business, and that all contractors and volunteers are bound to comply with this administrative procedure.

D. Pay the cost of ISP services or remote access connections that it approves for non-networked PCs.

E. Manage the configuration of anti-virus software for non-networked, County-owned PCs, and obtain from DTS any necessary anti-virus software.

F. Through DTS or departmental IT staff, ensure that the operating system on PCs have software updates in accordance with County information technology policies and procedures.

G. A Department head must seek approval from the CIO prior to monitoring or accessing an employee's electronically-stored email messages or computer files, or any other electronically-stored information available related to the employee's use of the County's Internet, intranet, and email services.

5.2 County Employees

A. Keep apprised of the latest version of this administrative procedure.

B. Ensure use of County-provided Internet, intranet, and email services is in accordance with this administrative procedure.

C. Must not access another user's email account without authorization from the department director or the employee to whom the email account is assigned.

D. Obtain department approval prior to acquiring a County-provided ISP connection for a non-networked PC.

E. In accordance with County information technology policies and procedures, obtain approval from the CAO before sending a broadcast email to all, or the majority of, County email users.

PROCEDURE

6.0	Employee	Abide by this administrative procedure as it relates to the use of Internet, intranet, and email services.
6.1	Department	Ensure that all employees are informed of and abide by this administrative procedure.

ISP Connection on Non-Networked Computer

6.2	Employee	Request approval from department for the acquisition of a County-provided ISP connection for a non-networked PC.

6.3	Department	Approve or disapprove of the employee's request for a County-provided ISP connection for a non-networked PC. Pay the costs of any approved ISP services that result from the employee's request.

Broadcast email

6.4	Employee	Request approval from department for sending a broadcast email to all, or the majority of County employees.
6.5	Department	Request approval from the CAO prior to permitting an employee to send a broadcast email to all, or the majority of, County employees.
6.6	CAO	Approve or disapprove requests to send County-wide broadcast email messages.

Monitoring and Accessing Use

6.7	Department	Determine if there is a legitimate business purpose to monitor an employee's use of County-provided Internet, intranet, and email services, or to access an employee's email messages or computer files. If there is a legitimate business purpose to monitor an employee's use of County-provided Internet, intranet, and email services, the department head must request in writing to the CIO for approval to monitor an employee's use of County-provided Internet, intranet, and email services or to access an employee's email messages or computer files.
6.8	CIO	Approve or disapprove a department head's request for monitoring or accessing an employee's email messages or computer files.
6.9	DTS	For approved requests, provide appropriate information to the requesting department head.

DEPARTMENTS AFFECTED

7.0 All County Departments.

PURPOSE

1.0 To establish a procedure that ensures the County's electronic data assets are protected from theft, unauthorized destruction, use, modification, or disclosure.

DEFINITIONS

2.0 Access Point – This is a means of connection between networks, or between a network and a user device. Some examples of an access point are a wireless hub or device, a modem, a cable modem, a DSL (Digital Subscriber Line) connection, an ISDN (Integrated Services Digital Network) line, A VPN (Virtual Private Network) service, and a router or other device with more than one network interface between two or more subnets.

2.1 Computer Security Guideline - A document that defines security procedures and standards, which is located under the on-line address at: http://portal.mcgov.org/dpttmpl.asp?url=/content/departments_intranet/DTS/PolicyProcs/index.asp

2.2 County Information Resources – A Montgomery County-owned, leased, or licensed computer, peripheral, network, system, or software element or package, and information transmitted, received, or stored using a County-owned, leased or licensed computer, peripheral, network, system, or software element or package.

2.3 Department of Technology Services (DTS) - A department in the executive branch that is responsible for automated information systems and telecommunications technology for the County Government.

2.4 Disaster Recovery Guideline - A document that describes the Information Technology steps taken for a disaster recovery, which is located under the on-line address at: http://portal.mcgov.org/dpttmpl.asp?url=/content/departments_intranet/DTS/PolicyProcs/index.asp

2.5 Digital Subscriber Line (DSL) - A family of technologies that provide a digital connection over the copper wires of the local telephone network.

2.6 Extended Network – A permanent or semi-permanent physical extension of the County's computer network to a non-County facility that is used by County and non-County employees to access County Information Resources.

2.7 Incident Response Guideline - A document that describes the policy for handling security incidents, which is located under the on-line address at: http://portal.mcgov.org/dpttmpl.asp?url=/content/departments_intranet/DTS/PolicyProcs/index.asp

2.8 Information – Data stored, processed, or transmitted by or to a computer, Personal Data Assistant (PDA) or any other device.

2.9 Information Technology Staff – An employee who is responsible to deploy, manage, administer, program, maintain or dispose of the County's computers, peripherals, networks, or software. This does not include staff that simply uses a computer, peripheral, network, data, or software to complete a job responsibility.

2.10 Integrated Services Digital Network (ISDN) – Type of circuit switched telephone network system, designed to allow digital (as opposed to analog) transmission of voice and data over ordinary telephone copper wires, resulting in better quality and higher speeds, than available with analog systems.

2.11 Network – Transmission channels and all supporting hardware and software interconnecting the County's computers and peripherals.

2.12 Network Equipment – Goods necessary for network communications, including routers, hubs, switches, network Interface cards, firewalls, and bridges.

2.13 PC – Personal computer.

2.14 Peripheral – Any hardware device connected to a computer (e.g., a monitor, keyboard, printer, Universal Serial Bus device, plotter, disk or tape drive, graphics tablet, scanner, joy stick, or mouse).

2.15 Privileged Account – A logon identification to the network with access exceeding the standard access given to employees.

2.16 Redundant Array of Independent Disks (RAID) – a system of using multiple hard drives for sharing or replicating data among the drives.

2.17 Risk Assessment Guideline - A document that defines how to assess a risk to data or County Information Resource, which is located under the on-line address at: http://portal.mcgov.org/dpttmpl.asp?url=/content/departments_intranet/DTS/PolicyProcs/index.asp.

2.18 Sensitive Information – Any information considered sensitive by law or County policy, including criminal justice, payroll/personnel, client or patient medical information.

2.19 System – A set of hardware and software that processes data in a meaningful way. A relatively simple computer system is a personal computer (PC).

2.20 System Administrator – An employee, either from DTS or another department, who is responsible for assigning and maintaining access rights (approvals) for privileged accounts.

2.21 Virtual Private Network (VPN) – A VPN is a network that uses encryption and other security methods to create a secure network on top of a non-secure and often public network.

POLICY

3.0 An employee must protect information resources commensurate with its level of sensitivity and applicable legal and County policy mandates for that particular type of information.

3.1 An employee must limit private use during his or her access to a County Information Resource, and normally use County Information Resources only to complete his or her work-related responsibilities.

3.2 A County Information Resource must have adequate environmental protection and safety systems, in accordance with manufacturer recommendations.

3.3 An employee may remove a County Information Resource from the County's premises only for business purposes and only upon the approval by appropriate personnel within the employee's department in custody of such resources.

3.4 Information that is critical to the County's operations must have regular backups and off-site storage. A department is responsible for having a critical County Information Resource disaster recovery plan, to provide for continuity of critical business operations and service delivery, in accordance with published DTS operating standards. The department must test the systems covered by the disaster recovery plan on a regular basis.

3.5 An employee and/or a department must follow the requirements listed under Paragraph 4.31 of this administrative procedure to have remote access to County Information Resources.

3.6 A County employee who violates this administrative procedure may be subject to disciplinary action, in accordance with Montgomery County laws and executive regulations, including Personnel laws and regulations, and Ethics Laws, currently codified at Chapter 33, COMCOR Chapter 33, and Chapter 19A of the County Code, respectively, and applicable collective bargaining agreements, as amended. Violation of this procedure is prohibited and may lead to disciplinary action, including dismissal, and other legal remedies available to the County.

3.7 In any contract where a contractor or business partner may have remote access to, or otherwise work on or interface with, County Information Resources, including those situations described below in paragraphs 4.11 (G), 4.12, 4.14 (E), 4.30, 4.31 (E) and 5.1 (C), the following language, or language of similar import, must be included in the solicitation document and the contract, and AP 6-7 must be attached:

This Contractor may be afforded remote access privileges to County information resources, or otherwise work on or interface with County information resources, and must ensure that the County's information resources, including electronic data assets, are protected from theft, unauthorized destruction , use, modification, or disclosure as deemed necessary under the County's Information Resources Security Procedure (AP 6-7). The Contractor must adhere to any and all policies and procedures under, or related to, the County's Information Resources Security Procedure (AP 6-7), which is expressly attached to, incorporated by reference into, and made a part of, this contract.

GENERAL

4.0 DTS must configure and install all access points connected to a County Information Resource.

4.1 DTS must install County network access controls (e.g., firewalls, boundary routers, etc.) to protect County Information Resources.

4.2 DTS will perform periodic (e.g., daily, bi-annual, etc.) security vulnerability audits on all County Information Resources in accordance with this administrative procedure.

4.3 Any Information or Information Resource that is contained in or stored on County Information Resources, or transmitted or received using County Information Resources, is the property of the County and, therefore, is not considered private.

4.4 The following are required to protect the identification and authentication of users of a County Information Resource:

A. Employees must, at a minimum, use identification controls and individual access accounts with passwords, to gain access to a County Information Resource.

B. Employees must not share identification controls.

C. Employees must limit privileged account use to specific functions, e.g. loading software, and may not be used on a continual basis apart from the intended function.

D. Account lockout procedures must conform to County Computer Security Guidelines.

E. DTS must terminate an employee's access to County Information Resources, immediately, when the employee is no longer employed in County service, or when an employee's responsibilities no longer require access to County Information Resources. DTS must terminate a contractor's access to County Information Resources, immediately, when the contractor's services is no longer required. Departments have this same responsibility for computer/device accounts under their control.

F. DTS must test password quality on a periodic basis. If a password is found to be weak as defined in the Computer Security Guideline the user must change the password.

G. Departments must disable any unused network logon ids.

4.5 The following are requirements to protect Sensitive Information:

A. An employee must not store Sensitive Information on a PC, unless DTS-approved PC security software is installed in the PC. A current list of DTS-approved PC security software is contained in the County Security Guidelines.

B. DTS may enable an employee to have access to Sensitive Information, only on the condition that the employee requires that Sensitive Information to perform the employee's responsibilities for the County.

C. An employee who has Sensitive Information stored on electronic media, or in any physical format, such as paper or fiche, is responsible for locking the information in a secure area when not in use, and deleting, reformatting, or shredding that Sensitive Information when it is no longer needed.

D. After using a PC terminal, an employee must not leave the PC terminal while Sensitive Information is displayed on the screen. An employee must never leave Sensitive Information on the computer terminal unattended; if necessary the department must install a screen-locking feature on the PC that blanks the screen until the correct password is entered.

E. The warning banner, as described in the County Security Guidelines, must be displayed on monitors, before employees are granted permission to access the computer system. An employee must have explicit permission from DTS in order to access or configure a computer device. All activities performed on a County Information Resource may be logged.

4.6 DTS requires that an information system joining the County network meet minimum security requirements as defined in the Computer Security Guidelines, unless an exception is granted by DTS.

4.7 The following are requirements when installing software security upgrades on County Information Resources:

A. A department is responsible for applying critical security patches, specified by the software vendor, for computer systems within 30 days after public release. For systems containing Sensitive Information or systems accessible via the Internet, a department is also responsible for applying critical security patches, within seven days of public release.

B. During emergency situations, the DTS Security Office may require that all computer systems immediately receive patches.

C. Departments must apply non-critical security patches to all County Information Resources other than computer systems within 90 days after public release.

D. If, due to incompatibility or other issues, a critical security patch cannot be applied, a department must submit an exception report, in writing, to the DTS Security Office.

E. The DTS Security Office must periodically verify software revision and patch levels for all County systems.

4.8 The following are requirements when using computer viral controls:

A. A department must install and run a DTS-approved, centrally administered, anti-virus application, using a DTS-approved configuration on all Information Resources that connect to the County network. A department must utilize the automatic updates, if available.

B. DTS and departments must protect County Information Resources by using an anti-virus program with virus definition no older than two weeks and having current approved software security updates applied to the County Information Resources.

4.9 The Department of Technology Services will do the following to audit County Information Resources:

A. Audit and review information resources on a regular basis, based on the sensitivity of the information or systems.

B. Log, and keep for a period of at least one year, records of unauthorized attempts to access Sensitive Information.

4.10 A department must install and run a DTS-approved, centrally administered, anti-spyware application, using a DTS-approved configuration on all Information Resources that connect to the County network. A department must utilize the automatic updates, if available

4.11 The following are requirements when accessing a non-County controlled network from within the County's network:

A. The right to use remote access services must be in accordance with AP 6-1, Use of County-provided Internet, Intranet, and Electronic Mail Services.

B. Access to remote access services must comply with the remote network owner's security and use policies.

C. A user that requires, and seeks to obtain, a modem at his/her workstation for remote access must receive approval from the DTS Security Office.

D. Encryption and authentication of any County Information Resource is required, if Sensitive Information is to be transmitted over public phone lines, the Internet, or wirelessly.

E. Sensitive information may not be stored on non-County controlled resources unless the department follows DTS procedures, County Security Policy, and all Federal, State and County laws and policies.

F. All VPN clients or any tunneling devices installed within the County network must be approved by DTS Security Office.

G. In order for a contractor to be afforded remote access privileges, the contractor must follow the same security requirements detailed in this administrative procedure and any other County Information Resource procedures. A department must include the Information Resources Security requirements noted in this administrative procedure in, or attach this administrative procedure to and incorporate it by reference into, any contract to which this administrative procedure applies.

4.12 The following must be met for a contractor or business partner facility to work on an extended network:

A. All network connections between a contractor or business partner and the County must meet the same security requirements detailed in this administrative procedure and the Computer Security Guidelines. The contractor or business partner must agree to implement, comply with, and enforce all County security policies and guidelines. A department must include the Information Resources Security requirements noted in this administrative procedure in, or attach this administrative procedure to and incorporate it by reference into, any contract to which this administrative procedure applies.

B. Failure by contractor or business partner to maintain full compliance with the County's security policies may result in immediate termination of the connection, and may be the cause for cancellation of any contract between the County and the contractor/business partner.

4.13 A department must do the following for the vulnerability, assessment, and remediation of County systems:

A. Conduct risk assessments and remediation on County Information Resources on a regular basis, commensurate with the level of sensitivity of the information, according to the Risk Assessment Guideline.

B. Support DTS scans against common infrastructure, on a regular basis.

C. Remediate vulnerabilities on a timeline commensurate with the associated level of risk. (Refer to Incident Response Guideline).

D. Report all system or network installations to the DTS Security Office, prior to implementation.

E. Comply with County Computer Security procedures established by the DTS Security Office, when installing new software.

4.14 Departments must do the following to ensure the safety of County Information Resources and personnel.

A. Create policies and ensure compliance to physically secure work areas.

B. Locate all new computer and communications centers in an area unlikely to experience natural disasters, serious or man made accidents, and related problems. New and remodeled facilities must be constructed to protect against fire, water damage, vandalism, and other threats that may occur. The location of multi-computer or communications facilities should be selected to minimize risk of damage.

C. Develop computer centers in consultation with DTS and the Department of Public Works and Transportation.

D. Notify the Department of Public Works and Transportation if changes in facilities are needed or if changes to plans are required.

E. A department must include the requirements of this administrative procedure in any contract to which this administrative procedure applies.

4.15 The Department of Public Works and Transportation must do the following to ensure the safety of County Information Resources and personnel:

A. Use environmental controls, including those related to humidity, temperature, and lighting, to protect all equipment.

B. Install fire detection and suppression equipment, as required by County, Federal and State law.

C. Periodically, inspect environment and safety systems by qualified personnel.

D. Use electrical protections on County Information Resources, commensurate with the importance of the County Information Resource.

E. Ensure the area is structurally sound.

F Ensure a physically secure infrastructure envelope exists.

G. Develop computer centers in consultation with DTS.

4.16 Departments and the DTS Security Office must do the following to ensure that access to County Information Resources is secure, by taking measures that include the following:

A Physically restrict unauthorized personnel from accessing County buildings, computer labs, offices, and work areas containing County Information Resources, including related equipment.

B. Permit only authorized personnel to have access to servers and wiring closets.

C. Restrict access to magnetic tape, disk, and documentation libraries to only employees whose responsibilities require access to them.

4.17 A department must do the following when moving or removing County Information Resource equipment owned or managed by DTS:

A. A departmental director or designee must receive approval from DTS to remove County Information Resources, which may occur only for DTS-approved business purposes. A department must provide the reason(s), in writing, for moving or lending the equipment. A department that has received approval to remove equipment so it may be repaired provided the department complies with DTS-approved repair processes and retains a receipt for the equipment from the repair provider.

B. Do not relocate computer equipment without prior authorization from the appropriate DTS management and/or technical support staff.

C. Use a sign-out procedure, approved by information resource owners, for all shared resources.

4.18 A department must do the following when installing copyrighted software:

A. Not make, use or display unauthorized copies of licensed software on County Information Resources.

B. Periodically, take an inventory of all software to determine if the software is properly licensed.

C. If an illegal copy of software is found, promptly acquire a license for the software or delete the software from the system, immediately. Document the discovery, licensure, or deletion of any illegal copy of software found.

4.19 Violation of this administrative procedure may result in adverse consequences, including fines to the County by the Software and Information Industry Association, or an indemnification or disciplinary action against the responsible employee.

4.20 A user of County Information Resources must not disable or modify security measures installed on any computer for any reason, without permission from appropriate DTS staff.

4.21 A user of County Information Resources must be trained in information security awareness, security threats, organizational policy issues, and the security aspects of the specific systems that the employee's department uses.

4.22 A department must do the following when designing or repairing a network server:

A. Place service contracts with the hardware vendor for repair/service for critical production systems, if possible. Contracts must specify response times for service, if possible.

B. Use backup or failover devices for critical network systems, if possible.

C. Place back-ups of County Information Resources at a physically separate, environmentally-controlled facility.

4.23 A department is responsible for the following when backing up County Information Resources:

A. Back-up crucial data and files frequently, and retain at least the last three back-up copies. The backing up of data is to be commensurate with the frequency of change of the data and the importance of recovering the lost data in a timely manner.

B. Back-ups must be at a physically separate, environmentally controlled facility.

C. All media used to store sensitive, valuable, or critical information for longer than six months must not be subject to rapid degradation. This information must be copied to newer media when the time limits suggested by the manufacturer are close to expiration.

D. Additional protections, such as RAID technology and hardware redundancy, should be used for appropriate, mission-critical applications.

4.24 A department is responsible for the following when establishing a disaster recovery plan for its data:

A. Develop a detailed disaster recovery and continuity of operations plan for County Information Resources.

B. A department that wishes to be supported by DTS, in the event of an emergency or disaster, must implement hardware and software policies and related procedures consistent with DTS standards. DTS staff is available to work with departments and offices to ensure compliance with DTS standards. (Refer to the Disaster Recovery Guidelines).

4.25 A department must develop a detailed plan to shut down each device in a computer center quickly, in the event of an emergency.

4.26 A department may be exempt from this administrative procedure under the following conditions:

A. The department must request exemption from this administrative procedure and receive written approval from the DTS Security Office. A detailed reason for the exception must be included, as well as the business purpose for the exception and additional precautions that will be taken to reduce the risk to the County network if the exception is granted. Examples of additional security precautions may include restricting Internet access and eliminating floppy disk and CD drives on the PC, or disconnecting from the County network.

B. A department that complies with the aforementioned section, and includes in its reason(s) for exemption that it has some older computer platforms in use that lack the capability to implement the security procedures outlined in this document. In this event, a department must purchase upgrades or replacements to these computer platforms as soon as possible, and, until this occurs, all Sensitive Information must be moved off these computers.

4.27 Employees may use County Information Resources only as follows:

A. For County business purposes, as provided under Paragraph 3.1 of this procedure and in accordance with AP 6-1, Use of Internet, Intranet, and E-mail Services, employees are responsible for using County Information Resources responsibly and to follow all related policies, regulations, security requirements, and laws.

B. Sign a confidentiality agreement in accordance with any policy, regulations, or laws.

C. Any use of County Information Resources, including the Internet, intranet, email, computers, or peripherals is subject to the County's review, copying, storing, archiving, and monitoring for violation of policies, regulations, and local, state or federal laws.

D. Montgomery County is not responsible for maintenance, damage, or loss of personally-owned computers, data, or peripherals used by employees in the work place.

4.28 An employee must use County Information Resources responsibly and professionally, and must not use County information resources in a manner that violates any federal, State of Maryland, or Montgomery County law, regulation, or policy, including this administrative procedure.

4.29 Employee orientations within the departments must include a requirement that employees take appropriate security precautions to protect County Information Resources, commensurate with the level of the employee's job, and the sensitivity level of the information the employee is required to use.

4.30 This administrative procedure applies to contractors, vendors, and volunteers who connect their computers to the county network. A department must include the requirements of this administrative procedure in any contract to which this administrative procedure applies. In addition all contractors, vendors and volunteers must comply with County Security Guidelines.

4.31 To have remote access to County Information Resources, an employee and/or a department must do the following:

A. An employee must receive written approval from the County Information Resource custodian and the DTS Security Office to have access County Information Resources from a non-County location, such as an employee's home or contractor's network. This written approval will be in an e-mail sent after the VPN request form is approved.

B. Before a department may purchase or install a remote access connection, the department must request and receive DTS Security Office approval, in writing, for the purchase or installation of a remote access connection.

C. Remote access of County Information Resources must be in accordance with AP6-1, Use of County-provided Internet, Intranet, and Electronic Mail Services.

D. Encryption and authentication of any County Information Resource is required, if Sensitive Information is to be transmitted over public phone lines, the Internet or wirelessly.

E. In order for a contractor to be granted remote access privileges, the contractor must follow the same security requirements detailed in this administrative procedure and any other County Information Resource procedures. A department must include this requirement in any contract to which this provision applies.

F. Sensitive Information may not be stored on non-County controlled resources unless following Department and DTS procedures and the County Security Guidelines and all Federal, State and County laws and policies.

RESPONSIBILITIES

5.0 Department of Technology Services

A. Maintain County information security policies appropriate for best business practices relating to the changing information security requirements of an enterprise network.

B. Conduct security scans and vulnerability testing to identify vulnerabilities in the County Information Resource network.

C. Advise departments on information security issues and assist them in the remediation of identified vulnerabilities.

D. Assist departments in the design of County Information Resource networks, to ensure a secure architecture.

E. Identify resources for security awareness training.

F. Function as the point of contact for County Information Resource-related security incidents.

G. Maintain an awareness of County Information Resource security threats and countermeasures.

5.1 Department

A. Become familiar with the County Information Technology Security Administrative Procedure.

B. Provide appropriate employees training to perform County Information Resource-related job functions, in compliance with County information technology security procedures.

C. Incorporate and include this administrative procedure as part of any contract in which the County is to provide a contractor or its agents or employees access to the County Information Resources network.

D. Cooperate with DTS staff in the vulnerability testing and remediation process of department-operated County Information Resources assets.

5.2 Employee

Use County Information Resources for County business purposes and in compliance with this administrative procedure.

PROCEDURE

6.0	Department of Technology Services	Provide departments with security policies and procedures and consulting expertise needed to maintain a secure and available County Information Resources network.
		Promote County Information Resources security awareness training.
		Scan the entire County Information Resources network periodically for known vulnerabilities and initiate remediation as required.
		Provide leadership in resolving County Information Resources security incidents and preventing incidents where possible.
6.1	Department	Enforce employee compliance with this administrative procedure.
		Train employees on department specific security policies and procedures.
		Assist DTS staff with maintaining the department Information Resources in a secure environment and in compliance with County security policies.

DEPARTMENTS AFFECTED

All County Departments.

APPROVED AS TO FORM AND LEGALITY.
OFFICE OF COUNTY ATTORNEY
BY Richard H. Melnick
DATE 4/25/05

Computer Security Guideline

Department of Technology Services

Revision Information

Effective Date: ___03_/_23_/_2009__

Last Revised Date: __03__/__23_/_2009__

Change History:

Changer/Author	Description/What Changed
Joan Cole	New policy statements to include Encryption for laptop hard drives, flash drives and portable external hard drives. Password requirement for Blackberry and other PDA devices.

Table of Contents

1. SCOPE 1

2. OVERVIEW 1

3. RESPONSIBILITIES 3

4. PHYSICAL SECURITY 4
- 4.1 Guideline 4
- 4.2 Environmental Requirements and Recommendations 4
- 4.3 Access to Work Areas 4
- 4.4 Removal of Equipment 5
- 4.5 Personnel Security 5
- 4.6 Disaster Recovery 6
- 4.7 Emergency Shutdown 6

5. DATA SECURITY 7
- 5.1 Guideline 7
- 5.2 Password and User-id Information 7
- 5.3 PDAs/Blackberry Password 8
- 5.4 Protection of Sensitive Information 8
- 5.5 Data Backup 8
- 5.6 Virus Control 9
- 5.7 Software Security Upgrades 9

6. SECURING PORTABLE DATA
- 6.1 Guideline 10
- 6.2 Laptop Hard Drive Encryption 10
- 6.3 USB Flash Drive Encryption 11
- 6.4 Portable/External Hard Drive Encryption 11

7. NETWORK SECURITY 10
- 7.1 Guideline 10
- 7.2 Remote Dial-in Access to County Computer Resources 10
- 7.3 Access from Remote Networks to County Computer Systems 10
- 7.4 Contractor Remote Access 10
- 7.5 Extended Networks 11
- 7.6 Vulnerability Assessment and Remediation 13
- 7.7 802.11 Wireless Access 13

8. CONDUCT AND USE 15
- 8.1 Guideline 15
- 8.2 Use of County Computer Resources 15
- 8.3 Adherence to Software Copyrights 15
- 8.4 Security Measures 15

9. EXCEPTIONS 15
- 9.1 Guideline 15

10. POLICY UPDATES 15
- 10.1 Guideline 15

1. SCOPE

The scope of this Computer Security Guideline includes all County owned or controlled computers (PCs, laptops, PDA's, wireless devices, servers, mini-computers, mainframe computers), all County owned or leased buildings, all data stored on those devices, all printouts, disks, tapes, or other media produced by those devices and all licensed software used on those devices. In addition, this Computer Security Guideline includes communications links to contractors and business partners and extensions of the County's computer network.

This Computer Security Guideline applies to all County employees, contractors, volunteers and persons legitimately affiliated with the County government for the efficient exchange of information and the completion of assigned responsibilities.

2. OVERVIEW

This Computer Security Guideline reflects accepted security controls taken from respected security and audit publications and adapted to Montgomery County's technical environment. These data security guidelines and standards have been developed to protect Montgomery County Government's electronic data assets from theft, destruction, and unauthorized use, modification, or disclosure. The loss of these assets could be very costly and disruptive to the County government. In today's computing environment, security controls are a necessity. The citizens of this County expect us to do what is prudent to protect the computing assets purchased with their tax dollars. Data is one of the most valuable assets of the County government. End-user computing dramatically increases the exposure for theft, corruption, loss, and misuse of County information resources since a larger number of people have access to data and data security controls. A significant percentage of direct access storage device capacity is installed outside the Computer Center. Security is an issue that cuts across all computing and organizational tiers. The implementation of security policies and procedures requires cooperation among users, managers, information systems personnel, security, audit personnel and most importantly, support from top management.

Access to the entire County's computing and communication resources is to be controlled based on the needs of the County and used for official County business only. Connection and access to computing resources is controlled through unique user identification (user-ids) and authentication (passwords). Each individual granted this privilege is responsible and accountable for work done under their unique identifier.

Computer users will be given access to a copy of the latest version of the Computer Security Administrative Procedure, this guideline, and the *Internet, Intranet, & Electronic Mail Administrative Procedure*. Individuals must adhere to the policies and are responsible for having the latest version of the Administrative Procedure. Refer to the *Internet, Intranet, & Electronic Mail Administrative Procedure* for additional information related to use of the Internet.

3. RESPONSIBILITIES

All Montgomery County Government computing and communication hardware, software, and data are considered to be "owned" by the Montgomery County Government.

The Department of Technology Services (DTS), in accordance with Montgomery County code section 2-58D, is responsible for protecting the integrity of the telecommunications network backbone, for operation and maintenance and security administration of the "enterprise" servers, mainframe and for maintaining the Computer Security Administrative Procedure and these guidelines. DTS is responsible for insuring that computer connections between County departments and with other government agencies are accomplished securely and as authorized.

Management in each department is responsible for ensuring that these computer security guidelines are enforced on the computing resources in their department. These security guidelines will be enforced for employees as well as for contractors and volunteers. Department management is responsible for providing pertinent information and notifying the DTS Security Team if a serious security breach occurs such as an intrusion, theft, or damage of computing resources. The operation, maintenance and security of de-centralized computing resources is the responsibility of department management in accordance with these guidelines.

The Local Area Network (LAN) administrator or decentralized IT staff is responsible for implementing the computer security guidelines described in this document on the servers in their department. LAN administrators will contact DTS network management for allocation of IP addresses.

As a user of data or computing resources or a custodian of those assets, everyone is responsible for data security.

4. PHYSICAL SECURITY

4.1 Guideline

Physical access to servers, individual PCs, and minicomputers will be protected from unauthorized persons. Personnel will not be put at risk of bodily harm.

4.2 Environmental Requirements and Recommendations:

A safe environment must be provided. Fire detection and suppression, and power and air conditioning are examples of the computer environmental protection and safety systems that must be provided.

- Areas with critical computer equipment must be equipped with fire and smoke alarms, and fire extinguishers.
- Critical equipment should be stored in a location that minimizes or prevents water damage due to leaking or flooding.
- Tall and top-heavy items must be stored in a manner anchored at to prevent damage or physical tipping.
- Items on wheels must have locking mechanisms to prevent rolling.

All equipment is to be maintained in a clean environment that meets or exceeds the manufacturer specifications related to temperature and humidity. Equipment areas should be kept free of obstructions. The cleanliness, environmental protection and safety systems are to be regularly monitored, and periodic inspections by qualified personnel should be scheduled. Electrical protection must be provided. Computer systems should have uninterruptible power supplies (UPS) and/or surge suppressors. All electrical wiring must meet state and local building codes. Preventive maintenance on computer and communications must be regularly scheduled. Preventive maintenance as defined by the manufacturer will help ensure that the risk of failure is minimized.

All new computer or communications centers must be located in an area unlikely to experience natural disasters, serious or man-made accidents, and related problems. New and remodeled facilities must be constructed to protect against fire, water damage, vandalism, and other threats that may occur. The location of multi-computer or communications facilities should be selected to minimize risk of damage. Locating such facilities above the ground floor will minimize the chances of water damage and theft. Kitchen facilities also must be located away from, but not directly above or below computer facilities. Due to potential water damage, restroom facilities should not be located directly above these facilities. Computer facilities should not be located adjacent to an exterior wall to protect the systems from unauthorized electromagnetic eavesdropping and damage from bombs.

DTS can provide the needed facilities more economically than creating a new computer center. If a new computer center needs to be created, contact the manager of the DTS computer center for requirements assistance. Local laws and ordinances must be considered when designing these locations.

4.3 Access to Work Areas:

Access to all buildings, computer labs, offices, and work areas containing computer-related equipment must be physically restricted and controlled. Access to servers and wiring closets must be restricted. Only authorized personnel will have access to wire closet/server areas. Authorized persons may include:

- DTS staff
- Outside contractors hired to work in these areas
- Building services and office staff at locations trained to reset equipment
- Fire and/or rescue personnel

Access to computer equipment must be supervised. Access to offices, computer rooms, and work areas containing sensitive information must be physically restricted. Managers responsible for employees working in these locations must determine the appropriate access controls. All multi-user computer and communications equipment such as fileservers, labs, and wiring closets must be located in locked rooms to prevent unauthorized usage.

Access to Server Centers or Network Operations Centers (NOCs) is restricted. Only employees whose job responsibilities require access to the client server center will be granted access. The supervisor of a server center or NOC is responsible for authorizing entrance and maintaining a list of those authorized to enter the facility.

Access to magnetic tape, disk, and documentation libraries must be restricted to employees whose responsibilities require access to them. The magnetic tape, disk, and documentation libraries housed within the controlled areas of the Server Center require additional precautions. This access is controlled by the supervisor of the Server Center.

Employees are not to permit unknown or unauthorized persons to enter restricted areas as they enter and exit these areas. Physical access controls for County buildings are intended to restrict the entry of unauthorized persons, and employees are expected to help restrict such access.

4.4 Removal of Equipment:

Permission to remove computers or related equipment may be granted only for accepted business purposes. Permission to remove computer equipment must be approved by the director of the department owning the equipment and the reason for lending the equipment must be put in writing stating the reason for which the equipment is loaned. Equipment being removed for needed repairs has implied permission when DTS approved repair processes are followed and a receipt is retained for the equipment.

PC equipment must not be moved or relocated without prior authorization from the appropriate management and/or DTS technical support staff. PC workstations, printers, peripherals, file servers, and electronics are examples of PC equipment covered by this requirement.

All County property must be returned when employees, consultants, or contractors terminate their relationship with County or with a specific work location within the County. It is the responsibility of the supervisor to collect County property from an employee leaving their location. Personnel terminating County employment or moving from one work location to another must inform their supervisor/administrator regarding County property they possess, and building access privileges.

When a computer support employee is involuntarily terminated, due care must be taken. Upon involuntary termination, the employee is to be immediately relieved of all duties and must return all County equipment and information. Their network accounts are to be immediately disabled and they are to be supervised while packing their belongings and leaving County facilities.

A sign-out procedure, approved by department management, must be utilized for laptop computers if there is a shared pool of laptops.

Montgomery County is not responsible for maintenance, damage or loss of personally owned computers or peripherals in the work place.

4.5 Personnel Security

Employees should contact building security if they feel threatened, harassed, or afraid of bodily harm.

Personnel will immediately contact building security if a person:

- becomes unruly
- refuses to leave
- poses a threat to employees, property, or equipment

In the case of an emergency, Montgomery County Police should be immediately contacted or dial 911. This is judgment decision based on the severity of the threat. If in doubt, contact the police first then building security.

4.6 Disaster Recovery

A detailed disaster recovery plan must be developed by each department that has a LAN or mini-computer. This plan will detail procedures to follow in the event of the loss of computing hardware, software and/or data. DTS must prepare, periodically update, and regularly review information technology emergency response plans for the DTS data center and for communications systems. The disaster recovery plan must provide for the continued operation of critical systems in the event of an interruption or degradation of service; must allow all critical computer and communication systems to be available in the event of a major loss, such as a flood, earthquake, or tornado; must prioritize the sequence of critical systems being recovered. This plan must be practiced at least once a year; this practice will include restoring data from backup media to insure that restoration procedures are known and to verify the integrity of the backup media. Each test must be followed by a report, and detail the test results, plus any remedial actions taken. The department can evaluate the effectiveness of the plan and make

adjustments as appropriate to accomplish the desired goals. The manager of the DTS data center can provide a comprehensive sample of a disaster recovery plan.

A business continuity analysis will also be conducted by those responsible for their department computing equipment that identifies the procedures that need to be in place in order to ensure that critical operations could continue in the event of a disaster which destroys their computing capabilities. The conditions that warrant a disaster declaration and the persons responsible for this decision will be specified.

Departments wishing to be supported by the DTS in the event of an emergency or disaster must implement hardware, software, policies, and related procedures consistent with DTS standards. DTS staff is available to work with offices to ensure compliance with DTS standards. Backup medium must be erased by following the *Data Backup* section in this guideline.

The communications networks should be designed without a single point of failure whenever possible, such as a central switching center, which could affect the availability of network services.

A backup of system wide critical information and software is to be stored in a physically separate, environmentally controlled facility. This facility is to be at least five miles from the site where original copies reside. Additionally, all current supporting materials such as manuals, charts, and diagrams needed for disaster recovery will be housed at the same facility. Supporting materials include anything required by County departments or units that are necessary to maintain day-to-day mission critical operations until recovery. Contact the DTS data center manager for information on the facility used by the data center for backups.

4.7 Emergency Shutdown Procedures

A detailed plan will be developed by each department with their own LAN or Mini-computer to shut down each device in a computer center quickly in the event of an emergency. Emergencies can include fire, loss of environmental controls, computer virus outbreak, natural disasters, etc. The goal is to preserve County resources in an emergency without subjugating the operator to undue risk. Contact the DTS data center manager for a sample of this plan. The DTS security manager or the director of the affected department can make this determination and contact the appropriate department management personnel to implement the emergency shutdown procedures when warranted by the circumstances. This kind of emergency will require every effort to shut down the computing equipment. Unplug the equipment from the County network if shutdown is not possible.

5. DATA SECURITY

5.1 Guideline:

Employees that are permitted access to computer systems must follow guidelines in order to insure that restricted access is maintained. Users of the computer systems will only have the minimal access needed to perform their tasks. Attempts to bypass security procedures to gain unauthorized access to computer resources are unacceptable and may result in disciplinary action. See section 3 paragraph 5 for information regarding disciplinary action.

5.2 Password and User-id Information:

Strong passwords will be used to protect access to County networked computer systems (LANs, mini-computers, PCs. Unused and default or installation user-ids will be disabled. Use of powerful user-ids such as those with system administrator attributes will be restricted.

Passwords provide a basic first-level security for restricting access to computer resources. To protect County computer resources properly, passwords are required to access all networked computer systems. Passwords will be simple enough to memorize but unique enough to remain secret. Passwords will not be attached to a terminal or other public place where they are easily compromised. Passwords will not be associated with the current date or a person's name, hobby, or family. Good passwords are not found in the dictionary, contain numeric as well as alphabetic characters, and will be at least eight characters in length. Passwords will not be imbedded in user's automatic sign-on procedures unless approved by that department's management for procedures where it is required. Passwords cannot be changed in less than 2 days.

A maximum of ninety days between password changes is required for network, server and mini-computer access. The change interval for power on passwords for PCs, if used, is at each department's discretion. Where possible, password change will be

controlled automatically by security software. Passwords will be individually maintained to ensure confidentiality and individual accountability. Passwords will not be shared with others. If multiple people must share a user-id and password for a sound business reason, refer to the exception procedures in section 8 of this document. If it becomes necessary to give your password to a technical person to fix a problem you are experiencing, the password will be changed immediately after the problem is solved. An account will be suspended after no more than five invalid password attempts in a given day and remain suspended until an administrator can reactivate it. Passwords will not be reused for at least four password cycles. A user-id will be suspended after twelve months of non-use.

Access to computer resources will be terminated immediately for employees who leave County employment or when their responsibilities no longer require them to access those resources. Access will also be terminated immediately for contractors no longer requiring access to County computer resources. Department coordinators are responsible for deleting user-ids of people who have terminated, transferred out of the department, or no longer require computer access. If the department coordinator does not have access rights in order to remove or disable the account, then the coordinator must contact the DTS Security Office and E-messaging Directory Services Team.

Computer system security will prevent a user-id from being logged on in more than two different places at the same time. Just one user-id per computer platform will be assigned to an individual. System privileges, such as supervisory or system administrator attributes are sensitive and are restricted to designated LAN or minicomputer system administrators. When the use of sensitive system privileges is necessary by others (for example, during an on-site visit by field service engineers), the privilege will be immediately removed or the user-id disabled after the user is finished with the specific task.

DTS will test password quality on a periodic basis. If a password is found to be weak, the user will be required to change it.

5.3 PDAs/Blackberry Password:

All County issued Personal Digital Assistants (PDAs) or Blackberry devices configured to communicate with County network resources must be password-protected. Enterprise-wide system policy will enforce this policy when device is not in use or after 30 minutes of inactivity.

5.4 Protection of Sensitive Information

Sensitive information includes criminal justice, payroll/personnel, client or patient information and any other data considered confidential by law or departmental policy. Sensitive information will not be stored on a PC unless PC security software has been installed on that PC. Sensitive information should be stored on the mainframe or network server where better security is available to protect the integrity of this information. Access to this information will be restricted to those who have to use it. Examples of information that will be protected from unauthorized access include: word processing documents containing sensitive material, which can be locked (password protected); source code for programs, which can be protected using a source code management tool; databases, which can use built-in security controls; and production files downloaded from the mainframe or server, which can be protected in a directory where limited access is permitted.

Sensitive information stored on computer diskettes, tapes or printout will be locked in a secure area when not in use and deleted, reformatted or shredded when no longer needed.

The same level of security will be maintained across the various computer platforms (mainframe, mini, LAN or individual PC). If a sensitive file located on the mainframe computer is downloaded to an individual PC, that information on the PC will be protected from unauthorized access in an equivalent manner as it is on the mainframe.

PC’s and terminals will not be left unattended with the results of a query containing sensitive information displayed on the screen. If this is necessary, a screen locking feature that blanks the screen until the correct password is entered will be used. Sensitive printouts will not be left on an unattended printer.

Special care will be given for laptop or portable PC's. If possible, sensitive information will be stored on diskettes rather than the hard drive and in a separate secure location from the laptop. Some sensitive information may need to be encrypted in order to ensure adequate security. A power on password will be used. If the PC is lost or stolen, departmental security personnel and the DTS Security Team will be notified immediately, and a complete accounting of what was on that PC will be made.

If possible, unauthorized attempts to access sensitive information will be logged and kept for a period of at least one year. This is information that may be used as evidence in a criminal proceeding and must be protected.

Do not disclose user-ids, passwords or other sensitive information to anyone without verifying their authorization to have this information.

The following statement is wording that will be displayed to users before they are granted computer access. This warning banner will appear each and every time that someone logs into a County computer:

UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action and may be reported to law enforcement. There is no right to privacy on this device.

5.5 Data Backup:

Data and files that are crucial to the department's operations will be backed up and the retention of at least the last three copies is highly recommended. The frequency of backup is to be commensurate with the frequency of change and the criticality of recovering the lost data in a timely manner. Some data may need to be backed up daily; monthly backups in other cases may be sufficient. When possible, backups will be automated and take place during off-peak hours.

All archival back-up data that is stored off-site must be listed in a current log that shows the date when the information was last modified, as well as the content of the information. All media used to store sensitive, valuable, or critical information for longer than six months must not be subject to rapid degradation. This information must be copied to newer media when the time limits suggested by the manufacturer are exceeded.

Offsite storage facilities will be utilized for copies of backup files containing programs, data or transactions representing current County business that, if lost or destroyed, would be difficult or impossible to recreate. All backups will be retained a minimum of four weeks and at least two copies will be kept in offsite storage. Longer retention periods should be considered based on business requirements. Offsite storage facilities will also be utilized for files containing data with retention requirements imposed by county, federal or state government. Magnetic storage media provided by the offsite storage or disaster recovery facility for the purpose of restoring Montgomery County information will be thoroughly erased after being used. This may be done by programs designed to erase sensitive information or by reformatting the media at least 7 times.

Additional protections, such as mirror disks, RAID technology, and hardware redundancy should be used as appropriate for mission critical applications. Contact the DTS data center manager if you need assistance in setting up backup/restore procedures or need offsite storage procedures

5.6 Virus Control

Virus controls are necessary to prevent the spread of computer viruses to other computers in the network. Virus eradication can be very time consuming and result in the loss of service to the citizens of Montgomery County.

Software not purchased by the County (e.g. software from bulletin boards, software from home computers or any other computer or network), when allowed by County and department policy, will be checked for viruses before use. This includes diskettes, CD-ROMs and information downloaded from the Internet or other on-line services. Information downloaded to the hard drive will be checked immediately upon completion of the download. Diskettes and CD-ROMs received from other departments or agencies or from companies doing business with the County will be checked before use.

All those responsible for departmental computer resources will update those resources with anti-virus signatures on a minimum weekly basis and upgrade to the most current anti-virus release as it becomes available. All PC’s and servers that are connected to the county network must have DTS approved, centrally administrated anti-virus software installed and running using a DTS approved configuration. Automatic updates will be utilized if available. Contact the DTS Client Computer Services (DCM) if information is needed on anti-virus software. When DTS issues a security alert and specifies that virus signatures must be updated immediately, those responsible for departmental computer resources must comply.

5.7 Software Security Upgrades

Vendors publish patches and upgrades to their software when they discover security flaws that could allow computer security to be compromised. The DTS Security Team may provide information about enterprise software security issues and patches as available and appropriate.

Because these flaws pose a significant threat, critical security patches for internal computer systems must be applied in a maximum of 30 days after public release. For systems containing sensitive information or are accessible via the Internet, critical security patches must be applied within 7 days of public release. Automatic updates will be utilized if available. If alerted of a specific critical threat that could severely affect County resources, the DTS Security Office may issue a mandatory, short time frame alert to computer administrators to patch specific computer resource in order to reduce the risk of network down time.

Non-critical security patches must be applied to all systems within 90 days of public release.

If, due to incompatibility or other issues, a critical security patch cannot be applied, an exception report must be sent in writing to the DTS Security Office.

On a regular basis, the DTS Security Office will verify software revision and patch levels for all County systems. Refer to the *Vulnerability Assessment and Remediation* section for details.

6. SECURING PORTABLE DATA

6.1 Guideline:

The widespread use of portable computing devices or PDAs, such as the Blackberry, iPods, USB flash drives, etc. has also increased exponentially the threat of theft or loss of sensitive data. The goal is for the County to protect all sensitive data at rest or in transit

6.2 Laptop Hard Drive Encryption:

All primary laptops are supported by the Desktop Computer Modernization (DCM) program and are required to have hard drive encryption. All secondary departmental laptops assigned to specific users must also have hard drive encryption. All secondary laptops not assigned to an individual (shared) will not be required to be encrypted due to operational impacts. Therefore, no County data may be stored on shared laptops. Instead, data used on shared laptops must be stored on secure USB Flash drives.

6.3 USB Flash Drive Encryption:

County requires the use of encrypted USB flash drives. Department Directors must decide who can have such devices; what data will be allowed on these drives; and must cover the cost of acquisition.
For Non-Sensitive Data – Standard off the shelf USB flash bundled with 256 bit AES encryption must be used. For Sensitive Data – Standard off the shelf USB flash bundled with higher levels of encryption and with self destruct function must be used.

6.4 Portable/External Hard Drive Encryption:

Portable/ External Hard drives must be kept in a locked cabinet or drawer/office and must be encrypted if removed from County facilities. Department Directors must decide who can have such devices; what data can be stored on these drives; and enforce either physical security or require a device that has encryption.

7. NETWORK SECURITY

7.1 Guideline:

Access to or from the County network is only permitted for authorized employees and other County approved agencies.

7.2 Remote Dial-in Access to County Computer Resources:

Access to remote network services will be in accordance with the *Internet, Intranet, & Electronic Mail Administrative Procedure*. Approval from the department management and the DTS Security Office will be obtained if a user requires a modem at their workstation for remote access. Modems attached to PC's that are connected to a County network can be very risky and will not be authorized unless DTS-approved security measures are implemented. Unauthorized modems attached to PCs or servers that are connected to a County network are prohibited. If remote access from a County owned PC using an

attached modem is required, that PC will be disconnected from all LANs or networks. Refer to the *Internet, Intranet, & Electronic Mail Administrative Procedure* document.

7.3 Access from Remote Networks to County Computer Systems

Access from a remote site to any Montgomery County computer resource will be approved by the employee's Department head or designee and by the DTS Security Office. All remote access systems used to access County computing resources will be approved by the DTS Security Office prior to purchase, installation, or connecting to County resources. Access and security system information must not be disclosed to any 3rd party.

Employees who need remote access to any County computer resources will submit a request in writing to the DTS Security Office stating what the access is to be used for, how long the access is required, and approval from the responsible department official. Contact the DTS Security Office to obtain information and approval for secure remote access options including, but not limited to, VPN, and wireless methods. Modems attached to County computer systems that allow remote access is not an approved remote access method. The list of authorized remote access users will be reviewed periodically by the LAN or mini computer administrator to determine continued need for such access and accuracy of the list. If remote access is no longer required, that access will be terminated.

LAN and mini computer administrators will maintain a log of unsuccessful attempts to access County computers. This log will be maintained for one year.

Encryption of any County-owned data is required if it is to be transmitted over public phone lines, the Internet, or wirelessly. County approved remote access solutions already use encryption.

7.4 Contractor Remote Access

All contractors will meet the same security requirements detailed in this and all other related County documents. The contractor will agree to, and is responsible for, maintaining compliance with all County security policies. Virtual Private Network (VPN) is the current approved remote access method. The sponsoring Department head or designee and the DTS Security Office will approve the remote access request.

The department whose contractor requires remote access to the County's network will present a written justification to the DTS Security Office. All plans for establishing remote access will be approved by the DTS Security Office in advance of implementation. These plans will include at least the following:

Type of access
When and how long access will be required
Security procedures (how contractor access will be controlled)

All contractors requiring access will sign non-disclosure statements and agree to abide by all County security policies and procedures prior to receiving access.

7.5. Extended Networks

Extended Networks are permanent or semi-permanent physical extensions of the County's computer network to a non-County facility and used by non-County employees to access County computer resources.

All network extensions to a contractor or business partner facility will meet the same security requirements detailed in this and all other related County documents. The Contractor/Business Partner (C/BP) will agree to, and is responsible for, maintaining compliance with all County security policies.

The Department requesting the extended network will present a written justification to the DTS Security Office for granting a C/BP access to the County's network from a remote location.

The C/BP will provide a secure link (e.g., T-1) between the C/BP site and the County's Computer Center. All plans for establishing a link will be approved by the DTS Security Office in advance of installation. These plans will include the following:

Type of connection
How long connection will be required
Hours of operation

Number and type of workstations and servers at remote location
Physical security plan
Security Procedures (including keeping all security systems up-to-date)
Anti-virus procedures
Whether Internet access is required for any workstations
The process of disconnecting the C/BP once the connection is no longer needed

All material submissions mentioned above will be submitted by the Contractor / Business Partner to the County Department requesting the extended network, which will coordinate reviews and approvals with the DTS Security Office.

The C/BP will maintain all security provisions, detailed in this guideline, while the remote location is connected to the County network. All employees that have access will sign non-disclosure statements, receive security training, and agree to abide by all County Security Policies and procedures (sign County security agreement), prior to receiving access. All training materials will be approved by the DTS Security Office in advance.

A list of employees with authorized access will be kept up to date and provided in a monthly report to the DTS Security Office. Requests for additional staff access will be approved by the DTS Security Office or County contract administrator prior to granting the access.

The C/BP will permit the DTS Security Office to inspect the remote location without notice, at any time. This may include technical security scanning of the C/BP network segment and any system connected to it.

The C/BP network segment, defined as all workstations, servers, and network equipment connected to the County, will not also be connected to any other network (including the C/BP own internal network). Remote access to the C/BP network segment will NOT be permitted; dial-in or dial-out will not be allowed.

Failure to maintain full compliance with the County's security policies will result in immediate termination of the connection, and may be cause for cancellation of any contract between the County and the C/BP.

7.6 Vulnerability Assessment and Remediation

System/network administrators need to have a vulnerability assessment performed against their assets on a bi-yearly basis. All aspects of this guideline will be evaluated for risk assessment. The security manager will determine the exact schedule. The security manager may also define any additional security assessments other than those described here. In cases where networks reside behind firewalls, multiple assessments should be conducted from both the internal and external sides of the firewalls.

The security manager will be responsible for conducting scans against common infrastructure. The security manager may also conduct scans at random intervals provided that this activity doesn't interfere with business operations. In cases where loss of services might occur, the security manager will coordinate with the appropriate administrators/authorities prior to the assessment.

System/network administrators will only be allowed to scan segments that they're responsible for. Also, the security manager will determine what signatures and scanning methods will be allowed. If sufficient controls do not exist, then the security manager will conduct a scan on behalf of the administrator.

As a general rule, if a vulnerability assessment reveals high-risk vulnerabilities, administrators will have one week to make appropriate changes. Medium-risk vulnerabilities will be addressed within one month. The security manager will coordinate with administrators to adjust this timeline as necessary. If no working patch or configuration change exists or if it will cause an extended or re-occurring stop to business operations, the security manager will evaluate any alternatives or provide a waiver. If high risk vulnerabilities are not remediated within the allotted time, the system may be disconnected from the network. In any case, the security manager will be available to assist administrators in developing remediation solutions. Notify the security manager with results of the vulnerability assessment.

All system or network installations must be reported to the security manager prior to implementation. This should include the following:

New or changed network access points (RAS, VPN, wireless, etc.)
New or changed network segments
New or changed business applications

New or changed application/network servers

New installations must meet County Computer Security Administrative Procedure and be scanned for vulnerabilities using tools approved by the DTS Security Office prior to implementation.

7.7 802.11 Wireless Access

All wireless access points must be approved by the network manager or the security manager. A secure setup on these devices is critical and must be performed by the network team. All other wireless access points connecting to the County network are not permitted. Any existing wireless access points not setup by the network team must be disconnected immediately and the network manager notified to secure the wireless access appropriately.

8. CONDUCT AND USE

8.1 Guideline:

County computer systems should only be used in a legal manner.

8.2 Use of County Computer Resources

All use of computer facilities, networks, and technology resources are for County business purposes. Each user of these technology systems is accountable for using these systems responsibly, following all policies, regulations, security requirements, and laws. *Including the Montgomery County Personnel Regulations 2001 Section 5. Any Employee in violation of the aforementioned regulation will be subject to appropriate disciplinary action.*

As such, all electronic mail messages, files on personal computers or servers, or any information stored on or transmitted by County computers are subject to be reviewed, copied, stored, archived, and monitored for violation of policies, regulations, and local, state or federal laws. *Such employee shall be responsible for appropriate use of all County systems including the transmission to and from the County systems during work and non-business time.*

8.3 Adherence to Software Copyrights

No unauthorized copies of licensed software may be made or used. It is a violation of copyright and trade secret laws and licensing agreements to make or use unauthorized copies of any licensed software. An inventory of all software will be made periodically to determine if the software is properly licensed. Automated tools such as software metering may be used to ensure compliance with license agreements. If illegal copies of software are found, they are to be deleted from the system immediately or properly licensed to protect the County from litigation. This discovery and deletion will be documented.

8.4 Security Measures

Users are not to disable or modify security measures installed on any computer for any reason without permission from the appropriate staff. Security measures include such things as menu software, operating systems settings, and anti-virus software. If it is necessary to disable security to perform a hardware or software installation, security measures must be reactivated when installation is complete.

9. EXCEPTIONS

9.1 Guideline:

Exceptions to any of these guidelines must be approved by the department management and the DTS Security Office. Exceptions will be directed to DTS Security Office by departmental management, in writing or via email, for prompt consideration. A detailed description of the exception will be included as well as the business purpose for this exception and what additional precautions that could be taken to reduce the risk to the County network if the exception is granted. An example of additional security precautions may include restricting internet access and eliminating floppy disk and CD drives on the PC or disconnect from the County network.

There are some older computer platforms in use in the County which lack the capability to implement some of the security procedures outlined in this document. Upgrades or replacements to these computer platforms will be purchased as soon as

possible and until this occurs all sensitive information will be moved off these computers. These system exceptions must be documented in writing to the DTS Security Office.

10.0 Guideline Updates

10.1 Guideline:

The Computer Security Guidelines will be modified on as needed basis to reflect changes in our computing environment and deployment of new technologies. Updates or changes to this document will be communicated to County employees via e-mail and revised version will be posted on the County Intranet site.